PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-169048
(43)Date of publication of application : 13.06.2003

(51)Int.Cl. H04L 9/08
G11B 20/10
H04N 5/91

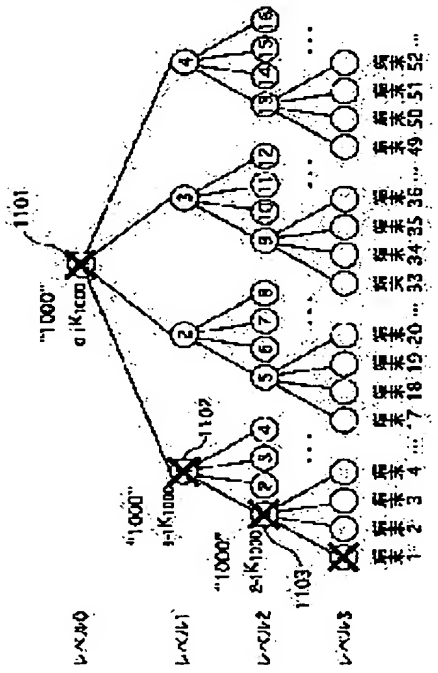
(21)Application number : 2002-089674
(22)Date of filing : 27.03.2002

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NAKANO TOSHIHISA
OMORI MOTOJI
MATSUZAKI NATSUME
TATEBAYASHI MAKOTO

(30)Priority
Priority number : 2001095730 Priority date : 29.03.2001 Priority country : JP
2001285608 19.09.2001 JP

(54) DATA PROTECTION SYSTEM FOR PROTECTING DATA THROUGH ENCRYPTION

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a system which suppresses an increase in the amount of encryption data to be distributed to many terminals and encrypts data so that the data can not correctly be decrypted on a specified terminal.
SOLUTION: For individual nodes except for those in the bottom layer in a quadrant tree wherein terminals are made to correspond to respective bottom- layer nodes, a plurality of combination patterns as to four nodes in layers which are reached from the nodes and one layer below them are determined, individual keys are determined by the combination patterns, individual keys are determined by the respective nodes in the bottom layers, and each terminal stores and holds all keys determined as to individual nodes on the corresponding path from the bottom layer node to the top layer. The individual nodes on the path from the node corresponding to a specified terminal (terminal 1) to the top layer are defined as ineffective nodes (mark '×' in Fig. 15) and keys determined corresponding to the combination patterns of all nodes except ineffective nodes among four nodes of the layer which is reached from the ineffective nodes other than the bottom layer and one stage below the layer are specified and used to cipher data to be distributed.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－169048
（P2003－169048A）
(43)公開日　平成15年６月13日(2003.6.13)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｇ１１Ｂ　20/10	Ｈ	５Ｃ０５３
Ｇ１１Ｂ　20/10		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｄ０４４
Ｈ０４Ｎ　5/91		Ｈ０４Ｎ　5/91	Ｐ	５Ｊ１０４

審査請求　未請求　請求項の数41　ＯＬ　（全 38 頁）

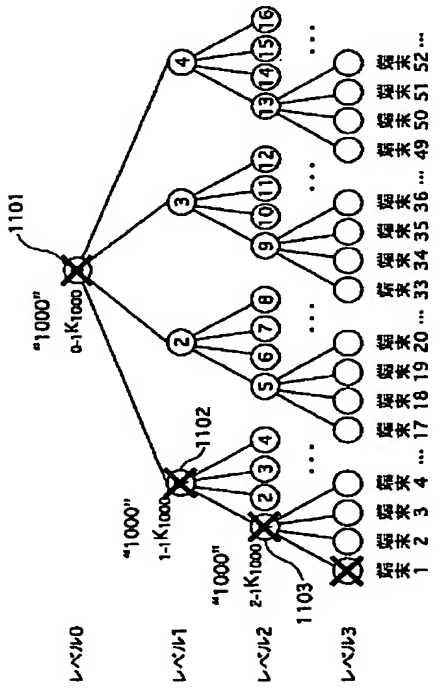
(21)出願番号　特願2002－89674(P2002－89674)
(22)出願日　平成14年３月27日(2002.3.27)
(31)優先権主張番号　特願2001－95730(P2001－95730)
(32)優先日　平成13年３月29日(2001.3.29)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2001－285608(P2001－285608)
(32)優先日　平成13年９月19日(2001.9.19)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　中野　稔久
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　大森　基司
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100090446
弁理士　中島　司朗

最終頁に続く

(54)【発明の名称】　暗号化を施すことによりデータを保護するデータ保護システム

(57)【要約】
【課題】　多数の端末に配給する暗号化データの量の増大化を抑制し、特定端末では正しく復号できないようにデータを暗号化するシステムを提供する。
【解決手段】　各端末を各最下層ノードに対応させた４分木の木構造で最下層を除く各ノードにつき、当該ノードから辿り着く１段下層の４個のノードについての複数の組合せパターンを決定し、組合せパターン毎に別個の鍵を定め、最下層の各ノード毎に別個の鍵を定め、各端末には対応する最下層ノードから最上層までの経路上の各ノードについて定めた全鍵を記憶保持させる。特定端末（端末１）に対応するノードから最上層への経路上の各ノードを無効ノード（図１５中×印）と定め、最下層以外の各無効ノードにつき、当該ノードから辿り着く１段下層の４個のノードのうち無効ノードを除く全てのノードの組合せパターンに対応し定めている鍵を特定し、特定した各鍵を用いて配給用データを暗号化する。



1

【特許請求の範囲】

【請求項１】　３台以上の端末、暗号化装置及び暗号化鍵特定装置を備え、各端末への配給用データを暗号化装置により暗号化して保護するデータ保護システムであって、

前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶しており、前記暗号化装置から出力された暗号化配給用データ群を取得して、暗号化配給用データを、記憶している復号鍵を用いて復号するものであり、

前記所定鍵割当方法は、

(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、

更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、

２つ以上の端末集合を決定し、

(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、

(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であり、

前記暗号化鍵特定装置は、暗号化鍵を特定する装置であり、かつ、

１つ以上の端末を無効化端末として特定する無効化端末特定手段と、

前記所定鍵割当方法により端末に割当てられた全ての復号鍵のうち無効化端末に割当てられた復号鍵以外の復号鍵を有効復号鍵と定めた場合において、

選定済みの有効復号鍵が割り当てられていない最も多くの端末に、割当てられている有効復号鍵を選定するという手順を、

選定済みの有効復号鍵が割り当てられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを有する装置であり、

前記暗号化装置は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成して出力する暗号化手段を有することを特徴とするデータ保護システム。

【請求項２】　前記所定鍵割当方法は更に、前記複数の端末集合を完全に包含する端末集合が存在するように、かつ、同じ１つ以上の端末集合を各々包含する複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決定を行う方法であることを特徴とする請求項１記載のデータ保護システム。

2

【請求項３】　前記所定鍵割当方法は更に、各端末集合が３台以上の端末を要素に含むように、かつ、３つ以上の端末集合を包含する端末集合が存在するように、端末集合の前記決定を行う方法であることを特徴とする請求項２記載のデータ保護システム。

【請求項４】　前記データ保護システムは、

各端末を各々別個の最下位層のノードに対応させた複数階層のＮ分木（Ｎは３以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなりＮ個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶している鍵記憶装置と、

前記所定鍵割当方法を実行し、前記各端末に割り当てる復号鍵群を決定する装置であり、かつ、

前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記鍵記憶装置により記憶されている復号鍵のうち、当該ノードの１段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記鍵記憶装置により記憶されている復号鍵とを、当該端末に割り当てるべきものとして決定する復号鍵決定装置とを備え、

前記各端末集合は、前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードからから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当するものであり、

前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、まず最上位層ノードを処理対象ノードとしておき、未処理の処理対象ノードが存在しなくなるまで暗号化鍵特定処理を繰り返し行い、

前記暗号化鍵特定処理は、未処理の１つの処理対象ノードについて、

(a) 当該処理対象ノードの１段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在する場合には、当該組合せパターンに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、

(b) 当該処理対象ノードの１段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在しない場合には、当該１段下位層が最下位層であれば当該１段下位層における無効ノード以外の全

てのノードに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該１段下位層が最下位層でなければ当該１段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、(c) 当該処理対象ノードの１段下位層において無効ノードが存在すれば、当該１段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることを特徴とする請求項３記載のデータ保護システム。

【請求項５】　前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項４記載のデータ保護システム。

【請求項６】　前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、Ｎ個全部の組合せ及び（Ｎ－１）個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項４記載のデータ保護システム。

【請求項７】　前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵それぞれについて、当該暗号化鍵を用いた暗号化により生成した暗号化配給用データと、前記鍵記憶装置により当該暗号化鍵に呼応する復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための暗号化鍵ノード識別情報とを、対応付けて出力し、

前記各端末は、所定鍵割当方法により個別に割当てられた各復号鍵を、前記鍵記憶装置により当該復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための復号鍵ノード識別情報と対応付けて記憶しており、前記暗号化装置から出力された暗号化配給用データ群及び暗号化鍵ノード識別情報群を取得して、当該端末が記憶している復号鍵ノード識別情報と一致する暗号化鍵ノード識別情報と対応する暗号化配給用データを、当該一致に係る復号鍵ノード識別情報と対応する復号鍵を用いて復号することを特徴とする請求項４記載のデータ保護システム。

【請求項８】　前記暗号化鍵特定装置は、

前記鍵記憶装置により記憶されている各復号鍵に呼応する暗号化鍵を記憶している暗号化鍵記憶手段を有し、

前記呼応する復号鍵と暗号化鍵とは互いに異なることを特徴とする請求項４記載のデータ保護システム。

【請求項９】　前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群をデータ記録媒体に記録することであり、

前記各端末は、前記暗号化装置により暗号化配給用データ群が記録されたデータ記録媒体から当該暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号することを特徴とする請求項１項記載のデータ保護システム。

【請求項１０】　前記暗号化手段は、

デジタル著作物であるコンテンツデータを記憶しているコンテンツ記憶部と、

乱数である前記配給用データを生成する乱数データ発生部と、

前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツデータを暗号化して、暗号化コンテンツデータを生成するコンテンツ暗号化部とを有し、

前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより、暗号化配給用データ群を生成して、当該暗号化配給用データ群と、前記コンテンツ暗号化部により生成された暗号化コンテンツデータとを前記データ記録媒体に記録し、

前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することを特徴とする請求項９記載のデータ保護システム。

【請求項１１】　前記データ保護システムは更に、

前記暗号化鍵特定装置により特定された暗号化鍵を特定するための暗号化鍵特定情報を、データ記録媒体に記録する暗号化鍵特定情報記録装置を備え、

前記各端末は、

乱数である前記配給用データを生成する乱数データ発生部と、

デジタル著作物であるコンテンツデータを格納しているコンテンツ格納部と、

前記データ記録媒体から暗号化鍵特定情報を読み出し、当該端末に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定部とを有し、

前記暗号化手段は、前記暗号化鍵選定部により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより暗号化配給用データ群を生成して、前記データ記録媒体に記録するものであり、

前記各端末は更に、
前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化して、暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化部と、
前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することを特徴とする請求項９記載のデータ保護システム。

【請求項１２】　前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群を前記各端末に送信することであり、
前記各端末は、前記暗号化装置により送信された暗号化配給用データ群を受信して取得し、暗号化配給用データを復号することを特徴とする請求項１記載のデータ保護システム。

【請求項１３】　暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定装置であって、
(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定し、
(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、
前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当手段とを備えることを特徴とする復号鍵決定装置。

【請求項１４】前記復号鍵設定手段は更に、前記複数の端末集合を完全に包含する端末集合が存在するように、かつ、同じ１つ以上の端末集合を各々包含する複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決定を行うことを特徴とする請求項１３記載の復号鍵決定装置。

【請求項１５】　前記復号鍵設定手段は更に、各端末集合が３台以上の端末を要素に含むように、かつ、３つ以上の端末集合を包含する端末集合が存在するように、端末集合の前記決定を行うことを特徴とする請求項１４記載の復号鍵決定装置。

【請求項１６】　前記復号鍵設定手段は、
各端末を各々別個の最下位層のノードに対応させた複数階層のＮ分木（Ｎは３以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなりＮ個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶しており、
前記復号鍵群割当手段は、
前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記復号鍵鍵設定手段により記憶されている復号鍵のうち、当該ノードの１段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記復号鍵設定手段により記憶されている復号鍵とを、当該端末に割り当てるべきものとして決定し、
前記各端末集合は、
前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードからから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当することを特徴とする請求項１５記載の復号鍵決定装置。

【請求項１７】　前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項１６記載の復号鍵決定装置。

【請求項１８】　前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、Ｎ個全部の組合せ及び（Ｎ－１）個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項１６記載の復号鍵決定装置。

【請求項１９】　暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定方法であって、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする復号鍵決定方法。

【請求項２０】　暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定処理をコンピュータに実行させるためのコンピュータプログラムにおいて、
前記復号鍵決定処理は、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とするコンピュータプログラム。

【請求項２１】　暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定処理をコンピュータに実行させるためのコンピュータプログラムを記録した記録媒体において、
前記復号鍵決定処理は、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする記録媒体。

【請求項２２】　暗号化されたデータを取得して復号するための３台以上の端末から構成される復号端末システムであって、
前記各端末は、
所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、
暗号化されたデータを取得する暗号化データ取得手段と、
前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段とを備え、
前記所定鍵割当方法は、
(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定し、
(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、
(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする復号端末システム。

【請求項２３】　前記暗号化データ取得手段は、前記暗号化されたデータをデータ記録媒体から読み出して取得することを特徴とする請求項２２記載の復号端末システム。

【請求項２４】　前記データ記録媒体には、暗号化鍵を

特定するための暗号化鍵特定情報が記録されており、
前記端末は更に、
乱数である鍵データを生成する乱数データ発生手段と、
デジタル著作物であるコンテンツデータを格納しているコンテンツ格納手段と、
前記データ記録媒体から暗号化鍵特定情報を読み出し、前記復号鍵群記憶手段に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定手段と、
前記暗号化鍵選定手段により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生手段により生成された鍵データを暗号化することにより暗号化鍵データ群を生成して、当該暗号化鍵データ群を前記データ記録媒体に記録する鍵データ暗号化手段と、
前記乱数データ発生手段により生成された鍵データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化することにより暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化手段とを備え、
前記暗号化データ取得手段は、前記データ記録媒体に記録されている暗号化鍵データ及び暗号化コンテンツデータを取得し、
前記復号手段は、前記暗号化データ取得手段により取得された前記暗号化鍵データを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号することにより鍵データを生成するものであり、
前記端末は更に、前記暗号化データ取得手段により取得された前記暗号化コンテンツデータを、前記復号手段により生成された鍵データを用いて復号するコンテンツ復号手段を備えることを特徴とする請求項２３記載の復号端末システム。

【請求項２５】　前記暗号化されたデータは外部の送信装置から送信されるものであり、
前記暗号化データ取得手段は、前記暗号化されたデータを受信することにより取得することを特徴とする請求項２２記載の復号端末システム。

【請求項２６】　３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定する暗号化鍵特定装置であって、
(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定し、
(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵群対応付け手段と、
前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵設定手段と、
１つ以上の端末を無効化端末として特定する無効化端末特定手段と、
前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、
選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、
選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることを特徴とする暗号化鍵特定装置。

【請求項２７】　前記復号鍵設定手段は更に、前記複数の端末集合を完全に包含する端末集合が存在するように、かつ、同じ１つ以上の端末集合を各々包含する複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決定を行うことを特徴とする請求項２６記載の暗号化鍵特定装置。

【請求項２８】　前記復号鍵設定手段は更に、各端末集合が３台以上の端末を要素に含むように、かつ、３つ以上の端末集合を包含する端末集合が存在するように、端末集合の前記決定を行うことを特徴とする請求項２７記載の暗号化鍵特定装置。

【請求項２９】　前記復号鍵設定手段は、
各端末を各々別個の最下位層のノードに対応させた複数階層のＮ分木（Ｎは３以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなりＮ個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶しており、
前記復号鍵群対応付け手段は、
前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記復号鍵設定手段により記憶されている復号鍵のうち、当該ノードの１段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記復号鍵設定

手段により記憶されている復号鍵とを、当該端末に対応付け、
前記各端末集合は、前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードからから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当し、
前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、まず最上位層ノードを処理対象ノードとしておき、未処理の処理対象ノードが存在しなくなるまで暗号化鍵特定処理を繰り返し行い、
前記暗号化鍵特定処理は、未処理の１つの処理対象ノードについて、
(a) 当該処理対象ノードの１段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在する場合には、当該組合せパターンに対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、
(b) 当該処理対象ノードの１段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在しない場合には、当該１段下位層が最下位層であれば当該１段下位層における無効ノード以外の全てのノードに対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該１段下位層が最下位層でなければ当該１段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、
(c) 当該処理対象ノードの１段下位層において無効ノードが存在すれば、当該１段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることを特徴とする請求項２８記載の暗号化鍵特定装置。

【請求項３０】　前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その各ノード（親ノード）について決定した全ての組合せパターンを、当該ノード（親ノード）から辿り着く前記Ｎ個のノードそれぞれを組合せ対象とするか否かを示す値を所定のノード順序に従って連結させてなる無効化パターン情報として当該ノード（親ノード）と対応付けて記憶するとともに、無効化パターン情報毎に別個の復号鍵を定めて、その定めた各復号鍵を当該ノード（親ノード）及び当該無効化パターン情報と対応付けて記憶し、
前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、最下位層を除く各ノードについて、当該ノードから辿り着く１段下位層のＮ個のノードそれぞれが無効ノードであるか否かを示す無効化情報を特定した後に、前記暗号化鍵特定処理を行い、
前記暗号化鍵特定処理は、未処理の１つの処理対象ノードについて、
(a) 当該処理対象ノードについて特定された無効化情報と整合する無効化パターン情報が存在する場合には、当該無効化パターン情報に対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、
(b) 当該処理対象ノードについて特定された無効化情報と整合する無効化パターン情報が存在しない場合には、当該１段下位層が最下位層であれば当該１段下位層における無効ノード以外の全てのノードに対応して前記復号鍵設定手段により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該１段下位層が最下位層でなければ当該１段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、
(c) 当該処理対象ノードの１段下位層において無効ノードが存在すれば、当該１段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることを特徴とする請求項２９記載の暗号化鍵特定装置。

【請求項３１】　前記復号鍵設定手段による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、Ｎ個全部の組合せ及び（Ｎ－１）個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該復号鍵設定手段は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることを特徴とする請求項２９記載の暗号化鍵特定装置。

【請求項３２】　３台以上の各端末への配給用データを暗号化する暗号化装置であって、
(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定し、
(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、
前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全

ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付け手段と、
１つ以上の端末を無効化端末として特定する無効化端末特定手段と、
前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、
選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段と、
前記暗号化鍵特定手段により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成する暗号化手段と、
前記暗号化手段により生成された暗号化配給用データ群を外部に出力する出力手段とを備えることを特徴とする暗号化装置。
【請求項３３】　前記出力手段は、前記暗号化鍵特定手段により特定された各暗号化鍵を識別するための鍵特定情報を前記暗号化配給用データ群とともに外部に出力することを特徴とする請求項３２記載の暗号化装置。
【請求項３４】　前記暗号化装置は更に、
デジタル著作物であるコンテンツデータを記憶しているコンテンツ記憶手段と、
乱数である前記配給用データを生成する乱数データ発生手段と、
前記乱数データ発生手段により生成された配給用データを鍵として用いて前記コンテンツデータを暗号化して、暗号化コンテンツデータを生成するコンテンツ暗号化手段とを備え、
前記出力手段は、前記コンテンツ暗号化手段により生成された暗号化コンテンツデータを前記暗号化配給用データ群とともに外部に出力することを特徴とする請求項３２記載の暗号化装置。
【請求項３５】　前記出力手段による前記出力は、前記暗号化配給用データ群をデータ記録媒体に記録することである。ことを特徴とする請求項３２記載の暗号化装置。
【請求項３６】　前記出力手段による前記出力は、前記暗号化配給用データ群を前記各端末に送信することであることを特徴とする請求項３２記載の暗号化装置。
【請求項３７】　３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための暗号化鍵特定方法であって、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、
１つ以上の端末を無効化端末として特定する無効化端末特定ステップと、
前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、
選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、
結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする暗号化鍵特定方法。
【請求項３８】　３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための特定処理をコンピュータに実行させるためのコンピュータプログラムであって、
前記特定処理は、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、
１つ以上の端末を無効化端末として特定する無効化端末

特定ステップと、
前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、
選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、
結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とするコンピュータプログラム。
【請求項３９】　３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための特定処理をコンピュータに実行させるためのコンピュータプログラムを記録した記録媒体であって、
前記特定処理は、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、
１つ以上の端末を無効化端末として特定する無効化端末特定ステップと、
前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、
選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、
結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする記録媒体。
【請求項４０】　３台以上の各端末への配給用データが、特定処理により特定された複数の暗号化鍵それぞれを用いて暗号化されてなる複数の暗号化配給用データを、記録したコンピュータ読み取り可能な記録媒体であって、
前記特定処理は、
前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、
更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、
２つ以上の端末集合を決定する端末集合決定ステップと、
端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、
前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、
１つ以上の端末を無効化端末として特定する無効化端末特定ステップと、
前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、
選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、
結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする記録媒体。
【請求項４１】　暗号化されたデータを取得して復号するための復号端末であって、
所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、
暗号化されたデータを取得する暗号化データ取得手段と、
前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段と、
前記所定鍵割当方法は、
(a) 本端末を含む３台以上の端末を想定した場合において本端末が、２つ以上の端末を要素に含む集合である複数の端末集合に属するように、
更に、本端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末

集合が存在するように、
２つ以上の端末集合を決定し、
(b) 本端末に対応して及び決定した端末集合毎に対応して各々別個の復号鍵を定め、
(c) 本端末に対して、本端末に対応して定めた復号鍵、及び本端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする復号端末。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データを複数の端末に暗号化して配給するデータ保護システムに関し、特に、データの暗号化及び復号に用いる鍵を決定する技術に関する。

【０００２】

【従来の技術】近年、マルチメディア関連技術の発展、大容量記録媒体の出現等を背景として、動画、音声等からなるデジタルコンテンツを生成して光ディスク等の大容量記録媒体に格納して配布するシステムが現れている。配布された光ディスク等に記録されているデジタルコンテンツは、コンピュータや再生装置等の端末において読み出されて、再生、コピー等の対象となる。

【０００３】かかるシステムにおいては一般的に、デジタルコンテンツに係るいわゆる著作権を保護するため、つまりデジタルコンテンツの不正コピー等といった不正利用を防止するために、暗号化技術が用いられる。即ち、かかるシステムは、デジタルコンテンツをある暗号化鍵を用いて暗号化して光ディスク等に記録して配布する。これに対し、その暗号化鍵に呼応する復号鍵を保持する端末のみが、光ディスク等から読み出したデータをその復号鍵を用いて復号して元のデジタルコンテンツを取得し、デジタルコンテンツの再生等を行うことができる。

【０００４】なお、デジタルコンテンツを暗号化して記録媒体に記録する方法としては、端末が保持している復号鍵に呼応する暗号化鍵でデジタルコンテンツそのものを暗号化して記録する方法や、デジタルコンテンツをある鍵で暗号化して記録した上で、その鍵に呼応する復号用の鍵を端末が保持している復号鍵に呼応する暗号化鍵で暗号化して記録する方法等がある。

【０００５】かかるシステムの一例として、例えば、「Ｎａｔｉｏｎａｌ　Ｔｅｃｈｎｉｃａｌ　Ｒｅｐｏｒｔ第４３巻第３号１１８頁～１２２頁」（松下電器産業株式会社　技術総務センター　平成９年６月18日発行）には、ＤＶＤ著作権保護システムが開示されている。このＤＶＤ著作権保護システムにおいて配布されたＤＶＤに記録されているデジタルコンテンツを再生するためのＤＶＤ再生端末は、その再生端末の製造メーカ毎に定められたマスタ鍵を予め保持しており、マスタ鍵を復号過程において用い、最終的にＤＶＤに記録されたデジタルコンテンツを復号し再生する機能を有する。なお、ＤＶＤには各メーカのマスタ鍵で暗号化された、デジタルコンテンツの復号用に必要となる鍵群が記録されている。

【０００６】

【発明が解決しようとする課題】ところで、通常、端末に保持されている復号鍵は秘密に保たれているが、端末の解析その他の方法で不正者が復号鍵を認識し暴露する可能性がある。ある端末に保持されている復号鍵が一旦暴露されてしまうと、不正者はこの復号鍵を用いてデジタルコンテンツの復号を行う端末やソフトウェア等を作成し、不正コピー等を行うおそれがあるので、結果的に、著作権保護のためには、暴露された復号鍵に呼応する暗号化鍵によりデジタルコンテンツを暗号化して光ディスク等に記録して配布することができなくなる。

【０００７】例えば、上述のＤＶＤ著作権保護システムに係るＤＶＤ再生端末について考えると、１つのＤＶＤ再生端末が不正に解析される等によって一旦マスタ鍵が暴露された場合には、それ以後そのマスタ鍵により暗号化したデジタルコンテンツの配布ができなくなる。この結果、その暴露以後にはＤＶＤの生成者等は、暴露されたのと別のマスタ鍵を用いた暗号化を施してデジタルコンテンツをＤＶＤに記録して配布せざるを得なくなるが、不正者に解析等されたＤＶＤ再生端末と同一メーカで製造された多数のＤＶＤ再生端末は、いずれも同じマスタ鍵を保持していることから、その暴露以後に新たに生成して配布したＤＶＤに記録されているデジタルコンテンツの復号及び再生を行えなくなるという問題が生じる。即ち、１つのＤＶＤ再生端末が不正者に解析等されると、多数のＤＶＤ再生端末が将来において新たに生成されたＤＶＤを利用できなくなってしまう。

【０００８】この問題を解決するために、ＤＶＤ再生端末毎に、別個の復号鍵を保持させておき、デジタルコンテンツ又はデジタルコンテンツの復号用に必要な鍵を、各ＤＶＤ再生端末の保持する復号鍵に呼応する各暗号化鍵を用いて暗号化して得られる全ての暗号化データをＤＶＤに記録する方法が考えられる。この方法によれば、一部のＤＶＤ再生端末が不正者に解析等され一部の復号鍵が暴露されても、それ以後においては、ＤＶＤ再生端末群に保持されている暴露されていない各復号鍵に呼応する各暗号化鍵を用いたデジタルコンテンツ等の暗号化により得られる全ての暗号化データをＤＶＤに記録して配布することができるため、暴露された復号鍵を保持するＤＶＤ再生端末以外の全てのＤＶＤ再生端末が、将来において新たに生成されたＤＶＤを利用することができるようになる。

【０００９】しかしこの方法も、ＤＶＤの配布対象として想定するＤＶＤ再生端末の数が膨大である場合には、ＤＶＤに記録すべき暗号化データが膨大になるという欠点を有する。そこで、本発明はかかる問題に鑑みてなされたものであり、デジタルコンテンツ、暗号化したデジ

タルコンテンツの復号に必要な鍵等のデータを暗号化して同一データを多数の端末に配給するデータ保護システムであって、配給対象の暗号化データの量の増大化をある程度抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにする暗号化技術を用いたデータ保護システムを提供すること、及びかかるデータ保護システムの構築に有用な技術を提供することを目的とする。

【００１０】

【課題を解決するための手段】上記目的を達成するために、本発明に係るデータ保護システムは、３台以上の端末、暗号化装置及び暗号化鍵特定装置を備え、各端末への配給用データを暗号化装置により暗号化して保護するデータ保護システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶しており、前記暗号化装置から出力された暗号化配給用データ群を取得して、暗号化配給用データを、記憶している復号鍵を用いて復号するものであり、前記所定鍵割当方法は、(a)前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であり、前記暗号化鍵特定装置は、暗号化鍵を特定する装置であり、かつ、１つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記所定鍵割当方法により端末に割当てられた全ての復号鍵のうち無効化端末に割当てられた復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が割り当てられていない最も多くの端末に、割当てられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が割り当てられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを有する装置であり、前記暗号化装置は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成して出力する暗号化手段を有することを特徴とする。

【００１１】ここで、配給用データは、記録媒体に記録されて配布され、或いは有線又は無線の通信路を通じて配信され、最終的に各端末に到達することが想定されるデータである。端末１、端末２、端末３を想定すれば、上述の所定鍵割当方法により決定される端末集合には、端末１及び端末２の組Ａや、端末１及び端末３の組Ｂや、端末２及び端末３の組Ｃがあり、所定鍵割当方法による割り当て結果を受けて端末１が記憶保持する復号鍵は端末１固有の復号鍵と、組Ａに対応する復号鍵Ａと、組Ｂに対応する復号鍵Ｂとであり、端末２が記憶保持する復号鍵は端末２固有の復号鍵と、組Ａに対応する復号鍵Ａと、組Ｃに対応する復号鍵Ｃとであり、端末３が記憶保持する復号鍵は端末３固有の復号鍵と、組Ｂに対応する復号鍵Ｂと、組Ｃに対応する復号鍵Ｃとである。この例において、端末２が不正に解析等されて端末２が記憶保持する全ての復号鍵が暴露されてしまった場合には端末２を無効化端末、つまり無効化にすべき端末として特定し、前記暗号化鍵特定手段による暗号化鍵の特定を行うと復号鍵Ｂに呼応する暗号化鍵が特定されることになる。

【００１２】従って、復号鍵Ｂに呼応する暗号化鍵を用いてデータを暗号化して各端末に配給すれば、端末２では正しくそのデータを復号することができず、端末１及び端末３では正しくそのデータを復号することができる。同様の目的を、端末１固有の復号鍵に呼応する暗号化鍵と端末３固有の復号鍵に呼応する暗号化鍵とをそれぞれ用いてデータを暗号化して各端末に配給することもできるが、この方法と比べて前述の復号鍵Ｂに呼応する暗号化鍵を用いる方法は、暗号化に用いる暗号化鍵の数が少なく、その分だけ配給される暗号化データのデータ量が少なくなるという効果を有する。

【００１３】即ち、本発明によれば、暗号化したデジタルコンテンツの復号に必要な鍵等のデータを暗号化して同一データを複数の端末に配給するデータ保護システムにおいて、配給対象の暗号化データの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにすることが可能となる。

【００１４】また、本発明に係る復号鍵決定装置は、暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定装置であって、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、前記各端末に対して、

前記復号鍵設定手段により当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当手段とを備えることを特徴とする。

【００１５】また、本発明に係る復号鍵決定方法は、暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定方法であって、前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする。

【００１６】また、本発明に係る復号端末システムは、暗号化されたデータを取得して復号するための３台以上の端末から構成される復号端末システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段とを備え、前記所定鍵割当方法は、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【００１７】また、本発明に係る復号端末は、暗号化されたデータを取得して復号するための復号端末であって、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段と、前記所定鍵割当方法は、(a) 本端末を含む３台以上の端末を想定した場合において本端末が、２つ以上の端末を要素に含む集合である複数の端末集合に属するように、更に、本端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 本端末に対応して及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 本端末に対して、本端末に対応して定めた復号鍵、及び本端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【００１８】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【００１９】また、本発明に係る暗号化鍵特定装置は、３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定する暗号化鍵特定装置であって、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵群対応付け手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵設定手段と、１つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることを特徴とする。

【００２０】また、本発明に係る暗号化装置は、３台以上の各端末への配給用データを暗号化する暗号化装置であって、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付け手段と、１つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段と、前記暗号化鍵特定手段により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成する暗号化手段と、前記暗号化手段により生成された暗号化配給用データ群を外部に出力する出力手段とを備えることを特徴とする。

【００２１】また、本発明に係る暗号化鍵特定方法は、３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための暗号化鍵特定方法であって、前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、１つ以上の端末を無効化端末として特定する無効化端末特定ステップと、前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする。

【００２２】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、暗号化に用いる暗号化鍵の数を比較的少なく抑えることができるので、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【００２３】

【発明の実施の形態】＜実施の形態１＞以下、本発明の実施の形態１に係るデータ保護システムについて図を用いて説明する。

＜全体構成＞図１は、本発明の実施の形態１に係るデータ保護システム１００の概略構成図である。

【００２４】データ保護システム１００は、同図に示すように、暗号化装置１０１、複数の復号装置（端末）１０３ａ～１０３ｎ及び鍵設定システム１０４を備え、映像、音声等を示すデジタルデータからなるコンテンツを暗号化してＤＶＤ－ＲＯＭ等である光ディスク１０２に記録して、複数の端末に配布するためのシステムである。

【００２５】ここで、鍵設定システム１０４は、暗号化装置１０１に設定するための暗号化鍵、及び復号装置１０３ａ～１０３ｎに個別に設定するための復号鍵を決定するシステムである。暗号化装置１０１は、鍵設定システム１０４により特定された暗号化鍵を保持しており、コンテンツを暗号化して、光ディスク１０２に記録する装置である。なお、光ディスク１０２については、完全に同一な記録内容を有する物が多数複製されることが想定される。

【００２６】また、復号装置１０３ａ～１０３ｎは、例えば１０億台といった多数の端末であり、各復号装置は、それぞれ個別に鍵設定システム１０４により決定された復号鍵を保持しており、光ディスク１０２から暗号化されたコンテンツ（以下、「暗号化コンテンツ」という。）を読み出して復号し、復号により得られるコンテンツを再生する装置である。

【００２７】なお、データ保護システム１００をコンテンツに係る著作権の保護を行うために用いる場合には、鍵設定システム１０４及び暗号化装置１０１は著作権保護の管理を行う機関に運用され、復号装置は一般ユーザ

に利用されることになると想定される。また、鍵設定システム１０４は、基本的に、各復号装置用の復号鍵を決定するために１度利用され、最初に用いられる暗号化鍵を特定するために１度利用され、更に、特定の復号装置が不正に解析される等によりその復号装置に保持されている復号鍵が暴露されたことが判明した都度、その特定の復号装置では光ディスクに記録された暗号化コンテンツの復号を行えないようにすることを目的として、暗号化装置１０１で新たにコンテンツを光ディスクに記録する際に用いられるべき新たな暗号化鍵を特定するために利用される。

【００２８】以下、暗号化装置１０１、復号装置１０３ａ～１０３ｎ及び鍵設定システム１０４について、より詳細に説明する。

＜暗号化装置の構成＞図２は、暗号化装置１０１及び復号装置１０３ａの機能構成図である。同図に示すように暗号化装置１０１は、コンテンツ記憶部２０１、乱数発生部２０２、暗号化鍵群格納部２０３、鍵暗号化部２０４、コンテンツ暗号化部２０５及び出力部２０６を有する。

【００２９】ここで、コンテンツ記憶部２０１は、映像、音声等を示すデジタルデータからなるコンテンツを記憶しているハードディスク等の記憶装置である。乱数発生部２０２は、コンテンツの暗号化に用いられる鍵（以下、「コンテンツ鍵」という。）となる乱数を発生する機能を有する。なお、コンテンツ鍵は、乱数からなる例えば６４ビットのデータである。

【００３０】暗号化鍵群格納部２０３は、鍵設定システム１０４により特定された１又は複数の暗号化鍵を格納し、また、格納している暗号化鍵に呼応する復号鍵を復号装置側が特定するために用いられる鍵特定情報を格納するメモリ等の記憶装置である。なお、鍵設定システム１０４の運用により新たに暗号化鍵の特定が行われた場合には、暗号化鍵群格納部２０３にその特定前に保持されていた暗号化鍵は削除され、新たに特定された暗号化鍵のみが暗号化鍵群格納部２０３に格納される。この新たな暗号化鍵及びその暗号化鍵に対応する鍵特定情報の格納は、例えばオペレータにより入力されることによってなされることとしてもよいし、鍵設定システム１０４からの受信によりなされることとしてもよい。

【００３１】鍵暗号化部２０４は、乱数発生部２０２から取得したコンテンツ鍵を、暗号化鍵群格納部２０３に格納された各暗号化鍵を用いて暗号化し、その結果である暗号化されたコンテンツ鍵（以下、「暗号化コンテンツ鍵」という。）それぞれを出力部２０６に伝える機能を有する。コンテンツ暗号化部２０５は、コンテンツ記憶部２０１に記憶されているコンテンツを、乱数発生部２０２から取得したコンテンツ鍵を用いて暗号化し、その結果である暗号化コンテンツを出力部２０６に伝える機能を有する。

【００３２】また、出力部２０６は、データを光ディスクに記録可能なハードウェアを含み、暗号化鍵群格納部２０３から鍵特定情報を取得し、その鍵特定情報と、コンテンツ暗号化部２０５から伝えられた暗号化コンテンツと、鍵暗号化部２０４から伝えられた暗号化コンテンツ鍵とを、光ディスク１０２へ記録する機能を有する。

【００３３】この暗号化装置１０１の記録により、光ディスク１０２には、暗号化コンテンツと、１又は複数の暗号化コンテンツ鍵と、鍵特定情報とが記録されることになる。なお、光ディスク１０２に記録される暗号化コンテンツ鍵の数は、鍵設定システム１０４により特定されて暗号化鍵群格納部２０３に格納されている暗号化鍵の数と一致する。

【００３４】このような暗号化装置１０１は、ハードウェアとしてはＣＰＵ、メモリ等を備えており、上述した乱数発生部２０２、鍵暗号化部２０４、コンテンツ暗号化部２０５及び出力部２０６の機能の全部又は一部はメモリに格納された制御用プログラムがＣＰＵにより実行されることにより実現されるものである。

＜復号装置の構成＞復号装置１０３ａは、光ディスク再生用の端末であり、図２に示すように取得部２１１、復号鍵群格納部２１２、復号鍵選定部２１３、鍵復号部２１４、コンテンツ復号部２１５及び再生部２１６を有する。

【００３５】ここで、取得部２１１は、光ディスクからデータを読み出し可能なハードウェアを含み、光ディスク１０２から暗号化コンテンツを読み出してコンテンツ復号部２１５に伝え、光ディスク１０２から暗号化コンテンツ鍵を読み出して鍵復号部２１４に伝え、光ディスク１０２から鍵特定情報を読み出して復号鍵選定部２１３に伝える機能を有する。

【００３６】復号鍵群格納部２１２は、鍵設定システム１０４により復号装置１０３ａに対して決定された複数の復号鍵等を格納する不揮発性メモリ等の記憶装置である。復号鍵の格納は、例えば復号装置の製造工程においてなされる。復号鍵選定部２１３は、取得部２１１から伝えられる鍵特定情報に基づいて、復号鍵群格納部２１２に格納されている復号鍵群のうちどの復号鍵を用いることができるかを判定し、用いることができる１つの復号鍵を選定する機能を有する。

【００３７】鍵復号部２１４は、復号鍵選定部２１３により選定された復号鍵を用いることにより復号可能な暗号化コンテンツ鍵を、取得部２１１を通じて取得し、取得した暗号化コンテンツ鍵をその復号鍵を用いて復号することによりコンテンツ鍵を生成する。コンテンツ復号部２１５は、取得部２１１から伝えられる暗号化コンテンツを、鍵復号部２１４により生成されたコンテンツ鍵を用いて復号することによりコンテンツを生成して再生部２１６に伝える機能を有する。

【００３８】また、再生部２１６は、コンテンツ復号部

２１５から伝えられたコンテンツを再生する機能を有する。なお、データ保護システム１００の扱うコンテンツが、例えばＭＰＥＧ（Ｍｏｖｉｎｇ　Ｐｉｃｔｕｒｅ　Ｅｘｐｅｒｔ　Ｇｒｏｕｐ）等で規定された圧縮方式に従った動画データであることとしたならば、再生部２１６は、例えば、いわゆるＭＰＥＧデコーダ等であって、コンテンツを伸長して映像信号を出力する機能を含む必要がある。

【００３９】このような復号装置１０３ａは、ハードウェアとしてはＣＰＵ、メモリ等を備えており、上述した取得部２１１、復号鍵選定部２１３、鍵復号部２１４、コンテンツ復号部２１５及び再生部２１６の機能の全部又は一部はメモリに格納された制御用プログラムがＣＰＵにより実行されることにより実現されるものである。

【００４０】なお、復号装置１０３ａ以外の複数の復号装置１０３ｂ～１０３ｎも、復号装置１０３ａと同様の構成を備える。但し、復号鍵群格納部２１２に格納されている内容の全部又は一部は復号装置毎に異なる。

＜鍵設定システムの構成＞図３は、鍵設定システム１０４の機能構成図である。

【００４１】同図に示すように鍵設定システム１０４は、鍵情報格納部３０１、鍵情報生成部３０２、無効化端末特定部３０３、鍵情報更新部３０４、復号鍵決定部３０５及び暗号化鍵特定部３０６を有する。ここで、鍵情報格納部３０１は、後述する鍵情報を格納するためのハードディスク等の記憶装置である。

【００４２】鍵情報生成部３０２は、データ保護システム１００を構成する復号装置それぞれを階層的な４分木の木構造の最下位層のノードに対応させるように木構造を決定し、木構造における各ノードについて１又は複数の鍵を割り当て、各ノードについて割り当てられた鍵等を示す鍵情報を生成する。なお、鍵情報は、暗号化鍵及び復号鍵を特定するために用いられるための情報であり、各ノードについて割り当てられた各鍵を暗号化鍵として用いることができるか否かの判断基準となる無効化情報を含む。この鍵情報及び４分木の木構造については後に詳しく説明する。

【００４３】無効化端末特定部３０３は、キーボード、ポインティングデバイス等の入力装置を介してオペレータから、保持している復号鍵が暴露された復号装置の指定を受け付け、その指定された復号装置を無効化すべき端末（以下、「無効化端末」という。）として特定する機能を有する。無効化端末は、コンテンツの暗号化において、その端末では暗号化コンテンツの復号が正しく行えないように、暗号化を行う必要がある復号装置を示す。

【００４４】鍵情報更新部３０４は、無効化端末特定部３０３により特定された無効化端末に基づいて、鍵情報格納部３０１に格納されている鍵情報中の無効化情報を更新する機能を有する。復号鍵決定部３０５は、鍵情報格納部３０１に格納されている鍵情報に基づいて復号装置それぞれについて設定すべき複数の復号鍵を決定する機能を有する。なお、各復号装置について決定された復号鍵は、その復号鍵について、鍵情報により対応付けられていたノードを示す情報とともにその復号装置の復号鍵群格納部に、例えば復号装置の製造工程において、格納される。従って、鍵設定システム１０４は、例えば、決定した復号鍵、及び復号鍵とノードとの対応を示す情報を例えば復号装置の製造用の製造システムに送信する。

【００４５】また、暗号化鍵特定部３０６は、鍵情報格納部３０１に格納されている鍵情報に基づいて暗号化装置に設定すべき１又は複数の暗号化鍵を特定する機能を有し、特定した暗号化鍵とノードとの対応を示すことにより復号時にどの復号鍵を用いるとよいかの判断基準となる鍵特定情報をその特定した暗号化鍵とともに出力する。

【００４６】この出力は、例えば、暗号化装置１０１への送信や、可搬性のある記録媒体への記録である。なお、暗号化鍵特定部３０６が暗号化鍵を可搬性のある記録媒体へ記録する場合には、運用上、オペレータによりその記録媒体の内容が暗号化装置１０１の暗号化鍵群格納部２０３にコピーされる必要がある。

＜鍵情報＞以下、鍵情報生成部３０２により生成され、鍵情報格納部３０１に格納される鍵情報について説明する。

【００４７】まず、４分木の木構造について説明する。図４は、４分木の木構造を示す図である。この木構造は、最下位層のノード群４０６を構成する各ノード（以下、「リーフ」ともいう。）と復号装置（端末）とが１対１で対応するように構築され、１つのノードからは４つのノードへの分岐を持つ木構造である。なお、ここでは、この１つのノードからｎ個のノードへの分岐を持つ構造をｎ分木と称しており、４個のノードへの分岐を持つ構造であれば４分木と称する。また、その４つのノードへの分岐を持つ１つのノードをその４つのノードに対して親ノードと称し、親ノードに対してその４つのノードを子ノードと称し、最上位層のノード４０５をルートと称することとする。

【００４８】データ保護システム１００における復号装置の数が、４の階乗数でない場合には、最下位層のノード数は、復号装置の数より大きい４の階乗数のうち最小の数となるが、ここでは、説明の簡単化のために、復号装置の数は最下位層のノード数と一致することとする。鍵情報生成部３０２は、図４に示す木構造の最上位層４０１をレベル０、１つ下の層４０２をレベル１と、順次１つ下の層をレベルを１つ増加して、最下位層の１つ上の層４０３をレベルＤ－１、最下位層４０４をレベルＤと定め、各レベルにおける各ノードは、各レベルにおける相対番号を１から順にそれぞれ定める。従って、レベ

ルＤにおける相対番号１のノードは復号装置１０３ａに対応し、レベルＤにおける相対番号２のノードは復号装置１０３ｂに対応し、レベルＤにおける相対番号４のＤ乗のノードは最後の復号装置１０３ｎに対応する。

【００４９】図５は、復号装置数が６４台である場合における４分木の木構造の例を示す図である。同図に示す例では、リーフが６４個存在するように４分木の木構造が構築されるため、最下位層はレベル３となる。次に、各ノードに対応して定める無効化情報について説明する。

【００５０】あるノードについての無効化情報は、そのノードを親ノードとした場合の４つの子ノードについて、そのノードが無効ノードであるか否かを示すフラグを、相対番号の小さいノードについてのフラグから順に結合した情報である。その、フラグは無効ノードであれば１、無効ノードでなければ０の値をとる。従って、例えば４つの子ノードが無効ノードでなければ親ノードの無効化情報は”００００”となり、４つの子ノードが無効ノードであれば親ノードの無効化情報は”１１１１”となる。

【００５１】但し、リーフについては無効化情報は、リーフに対応する復号装置が無効化端末であれば”１１１１”で無効化端末でなければ”００００”となることとする。なお、無効ノードとは、無効化端末に対応するリーフであるか、又は無効化端末に対応するリーフから上層に向けて辿り着くノードをいう。従って、無効ノードは、対応する無効化情報が”００００”以外の値をとるノードであるとも言える。

【００５２】ここで、特定のノードから「辿り着く」ノードとは、親ノードと子ノードとの関係にある各ノード間にはチェーンが張られていると想定した場合において、その特定のノードから上層方向及び下層方向のいずれか一方向に向けての１又は複数のチェーンにより、繋がっているノードをいう。従って、木構造において、上層のノードから終始下層方向に向けて１又は複数のチェーン上を通ることにより到達する下層のノードは、その上層のノードから辿り着くノードであり、逆にその上層のノードはその下層のノードから辿り着くノードである。例えば、いずれのリーフからもルートに辿りつき、ルートからもいずれのリーフに辿り着くが、あるリーフから他のリーフには辿り着くことはない。

【００５３】復号装置の保持する復号鍵が暴露される前においては、無効化端末は存在しないため、全てのノードについての無効化情報は”００００”の値をとる。図６及び図７は、ルートの無効化情報の例を示す図である。図６の例は、ルートの子ノードは全て無効ノードでない場合におけるルートの無効化情報は”００００”となることを示している。

【００５４】図７の例は、無効ノードを×印により示しており、ルートの子ノードのうち相対番号が１であるものだけが無効ノードである場合におけるルートの無効化情報は”１０００”となることを示している。次に、各ノードについて割り当てられる鍵について説明する。鍵情報生成部３０２により、各ノードについて別個に、暗号化鍵と、その暗号化鍵に呼応する復号鍵の組が割り当てられる。なお、リーフについては復号装置毎に固有の１組の鍵が割り当てられ、リーフ以外のノードについては以下に示すように複数組の鍵が割り当てられることになる。

【００５５】図８は、４分木の木構造のレベル０及びレベル１の階層のノードに対応して割り当てられる鍵を示す図である。同図中、０－１Ｋ００００、０－１Ｋ０００１等は、暗号化鍵及びそれに呼応する復号鍵を、便宜上まとめて表現したものである。なお、データ保護システム１００において暗号化鍵と復号鍵とは別個の値をとる方式又は同一の値をとる方式のいずれを採用するかを予め定めておくことができ、暗号化鍵と復号鍵とは別個の値をとる方式を採用する場合には、例えば０－１Ｋ０００００で表される復号鍵と０－１Ｋ００００で表される暗号化鍵は別個の値のものとなり、データ保護システム１００において暗号化鍵と復号鍵とは同一の値をとる方式を採用する場合には、例えば０－１Ｋ００００で表される暗号化鍵及び復号鍵は同一の値のものとなる。

【００５６】以下、各ノードには復号鍵が割り当てられているという表現又は各ノードには暗号化鍵が割り当てられているという表現を用いるが、実際には復号鍵と暗号化鍵とが別個の値をとる方式を採用する場合においては復号鍵とそれに呼応する暗号化鍵が各ノードに割り当てられており、復号鍵と暗号化鍵とが同一の値をとる方式を採用する場合においては、復号鍵でもあり暗号化鍵でもある鍵が各ノードに割り当てられていることになる。これにより、鍵情報中に割り当てられた復号鍵等が設定されることになる。なお、暗号化鍵及び復号鍵は、例えば６４ビットのデータである。

【００５７】図８に示すように、リーフ以外のノードについては、１１個の復号鍵が割り当てられている。ここでは、あるノードについての無効化情報のとり得る”００００”、”１０００”等の値のうち、”１”の数がｎ分木の木構造である場合における（ｎ－１）個未満となる値を無効化パターンと称する。従って、４分木における無効化パターンは、”１”の数が３未満となるところの”００００”、”０００１”、”００１０”、”００１１”、”０１００”、”０１０１”、”０１１０”、”１０００”、”１００１”、”１０１０”及び”１１００”の１１種類存在し、リーフ以外の各ノードには、全無効化パターン分の１１個の復号鍵が割り当てられている。

【００５８】ここでは、レベルＡの相対番号Ｂのノードについての鍵であって、無効化パターンがＸであるものを、「Ａ－ＢＫＸ」と表現している。従って「０－１Ｋ

０００００」は、レベル０の相対番号１のノードについての無効化パターンが”００００”に対応する復号鍵等であることを示している。図９は、鍵情報格納部３０１に格納される鍵情報の構成を示す図である。

【００５９】同図に示すように鍵情報５００は、各ノードについて、そのノードのノードＩＤ５０１と無効化パターン５０２と鍵５０３と無効化情報５０４とが対応付けられた情報である。ノードＩＤ５０１は、木構造におけるノードの所在位置を示すレベルと相対番号とを示すＩＤであり、例えばレベルＡの相対番号Ｂのノードのノードの ＩＤは「Ａ－Ｂ」と表現される。

【００６０】無効化パターン５０２は、上述のように無効化情報のとり得る値のうち”１”の数が３未満となる値である。鍵５０３は、対応するノードＩＤで示されるノードに割り当てられている復号鍵及び暗号化鍵である。無効化情報５０４は、対応するノードＩＤで示されるノードについての無効化情報であり、初期値は”００００”である。

【００６１】なお、鍵情報中、リーフに対応する無効化パターンはなく、リーフについての鍵５０３は１組の復号鍵及び暗号化鍵である。

＜鍵割当処理＞以下、鍵設定システム１０４における鍵情報生成部３０２により鍵情報格納部３０１に鍵情報が格納された後に、復号鍵決定部３０５が、全ての復号装置１０３ａ～１０３ｎそれぞれに設定すべき復号鍵を決定するために行う、即ち各復号装置に複数の復号鍵を割り当てるために行う鍵割当処理について説明する。

【００６２】図１０は、復号鍵決定部３０５により実行される鍵割当処理を示すフローチャートである。復号鍵決定部３０５は、まず復号装置（端末）のうち４分木の木構造におけるリーフの相対番号１が対応付けられた復号装置を割当対象端末とし（ステップＳ１１）、割当対象端末に対応するリーフ即ち最下位層のノードに着目してそのノード（着目ノード）に割り当てられている１つの復号鍵を特定する（ステップＳ１２）。なお、ノードへの着目とは、具体的には例えば、鍵情報中のそのノードについての情報の記憶領域内アドレスを内部処理用の変数等に格納すること等をいう。

【００６３】続いて、復号鍵決定部３０５は、着目ノードが有効であること即ち無効ノードでないことを示すところの、着目ノードの一層上のノード（親ノード）について、鍵情報格納部３０１に格納されている鍵情報において定められている無効化パターンに対応する復号鍵を全て特定し、その親ノードを新たに着目ノードと定める（ステップＳ１３）。

【００６４】ステップＳ１３に続いて、復号鍵決定部３０５は、現在の着目ノードはルートであるか判定し（ステップＳ１４）、ルートでなければ、現在の着目ノードがルートとなるまでステップＳ１３の処理を繰り返し行う。ステップＳ１４において現在の着目ノードがルートであれば、復号鍵決定部３０５は、割当対象端末に対してステップＳ１２及びステップＳ１３で特定した全ての鍵を設定すべき復号鍵として決定し（ステップＳ１５）、割当対象端末は、最後の端末か否か、即ち、リーフのうち相対番号が最も大きいものに対応付けられている復号装置か否かを判定し（ステップＳ１６）、最後の端末であれば鍵割当処理を終える。

【００６５】また、ステップＳ１６において割当対象端末が最後の端末でないと判定した場合には、復号鍵決定部３０５は、現在の割当対象端末の次ぎの端末、即ち現在の割当対象端末に対応するリーフよりも相対番号が１つ大きいリーフに対応付けられている復号装置を、新たに割当対象端末と定めて（ステップＳ１７）、ステップＳ１２の処理を行う。

【００６６】このような鍵割当処理により、各復号装置に対して設定されるべき復号鍵群が決定され、これを受けて、各復号装置はそれぞれ決定された復号鍵群を保持するように構成される。図１１は、６４台しか復号装置がないと仮定した場合においてレベル３の相対番号１のリーフに対応する復号装置（端末１）に割り当てられるものと鍵割当処理によって決定される復号鍵群９０５を示す図である。

【００６７】なお、同図中の３－１Ｋは、レベル３の相対番号１のリーフ９０４に唯一割り当てられている復号鍵を表したものである。６４台しか復号装置がないと仮定した場合においては、図１１に示すように、端末１には、レベル３の相対番号１のリーフ９０４に割り当てられている復号鍵３－１Ｋと、そのリーフの１層上の親ノードであるレベル２の相対番号１のノード９０３について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する復号鍵、即ち”００００”、”０００１”、”００１０”、”００１１”、”０１００”、”０１０１”及び”０１１０”という７つの無効化パターンに対応する７つの復号鍵２－１Ｋ００００、２－１Ｋ０００１、２－１Ｋ００１０、２－１Ｋ００１１、２－１Ｋ０１００、２－１Ｋ０１０１及び２－１Ｋ０１１０と、そのさらに１層上の親ノードであるレベル１の相対番号１のノード９０２について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する７つの復号鍵１－１Ｋ００００、１－１Ｋ０００１、１－１Ｋ００１０、１－１Ｋ００１１、１－１Ｋ０１００、１－１Ｋ０１０１及び１－１Ｋ０１１０と、そのさらに１層上の親ノードであるレベル０の相対番号１のノード即ちルート９０１について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する７つの復号鍵０－１Ｋ００００、０－１Ｋ０００１、０－１Ｋ００１０、０－１Ｋ００１１、０－１Ｋ０１００、０－１Ｋ０１０１及び０－１Ｋ０１１０との合計２２個の

復号鍵が割り当てられる。

【００６８】従って、この場合には端末１の復号鍵群格納部２１２にはその割り当てられた２２個の復号鍵が、例えば端末１の製造工程等において、格納されることになる。なお、リーフ以外の各ノードに対応する無効化パターンは、そのノードの子ノードが無効ノードであれば”１”を無効ノードでない有効ノードであれば”０”を、子ノードのレベル内相対番号の小さい順に連結した情報であり、無効化パターンに復号鍵を割り当てることは、無効化パターンにおいて有効ノードと示される全ての子ノードから辿り着くことのできる全てのリーフに対応する全端末を要素とする端末集合に対して復号鍵を割り当てることに相当する。従って、各端末には、その端末固有の復号鍵と、その端末を含む全ての端末集合に割り当てられている復号鍵とが割り当てられることになる。

【００６９】＜暗号化鍵の特定＞鍵設定システム１０４の暗号化鍵特定部３０６は、無効化端末がない状態、即ちどの復号鍵も暴露されていない状態においては、ルートに割り当てられている暗号化鍵０－１Ｋ００００、つまり復号鍵０－１Ｋ００００に呼応する暗号化鍵を、暗号化装置１０１の暗号化鍵群格納部２０３に設定すべき暗号化鍵として特定する。

【００７０】これに対し暗号化装置１０１は、この特定された暗号化鍵と、木構造におけるルートに割り当てられている復号鍵０－１Ｋ００００を特定する鍵特定情報とを、鍵設定システム１０４から受信する等によって、暗号化鍵群格納部２０３に格納している。光ディスク１０２へコンテンツを記録する場合には、暗号化装置１０１は、乱数発生部２０２から生成されたコンテンツ鍵を、暗号化鍵群格納部２０３に格納している暗号化鍵を用いて鍵暗号化部２０４において暗号化し、その暗号化により得られる暗号化コンテンツ鍵を鍵特定情報と対応付けて、出力部１０２により光ディスク１０２に記録し、また、コンテンツ鍵を用いてコンテンツ記憶部２０１に記憶されているコンテンツをコンテンツ暗号化部２０５において暗号化し、その暗号化により得られる暗号化コンテンツを出力部１０２により光ディスク１０２に記録する。

【００７１】以下、鍵設定システム１０４における鍵情報更新部３０４により実行される無効化情報更新処理について説明する。無効化端末特定部３０３により無効化端末が特定された場合に鍵情報更新部３０４は、鍵情報格納部３０１に格納されている鍵情報のうち、無効化端末に対応する４分木の木構造におけるリーフについての無効化情報を”１１１１”にして、そのリーフが無効ノードであることを示すようにした後に、鍵情報のうち各ノードに対応する無効化情報を更新する無効化情報更新処理を行う。

【００７２】図１２は、鍵情報更新部３０４により実行される無効化情報更新処理を示すフローチャートである。まず、鍵情報更新部３０４は、４分木の木構造における最下位層の１層上の層に着目する（ステップＳ２１）。つまり、最下位層がレベルＤであれば、レベル（Ｄ－１）の層に着目する。

【００７３】続いて鍵情報更新部３０４は、着目している層（着目層）の各ノードに相対番号の小さい順に順次着目し、その着目しているノード（着目ノード）の４つの子ノードについての無効ノードの組合せパターンに合致するように、着目ノードについての無効化情報を更新する（ステップＳ２２）。例えば、着目ノードの４つの子ノードが相対番号の小さい順に、「無効ノード」、「無効ノードでない」、「無効ノードでない」、「無効ノードでない」ものであった場合には、着目ノードについての無効化情報は”１０００”となる。

【００７４】ステップＳ２２の後に、鍵情報更新部３０４は、現在の着目層は最上位層即ちレベル０の層であるかを判定し（ステップＳ２３）、最上位層でなければ、着目層の１つ上の層に着目し（ステップＳ２４）、ステップＳ２２の処理を行う。鍵情報更新部３０４は、ステップＳ２３の判定において、現在の着目層が最上位層になるまで、ステップＳ２２～Ｓ２４を繰り返し、ステップＳ２３の判定において現在の着目層が最上位層になれば、無効化情報更新処理を終える。

【００７５】この結果として、４分木の木構造において無効化端末に対応するリーフから上層に向けて辿ると到達できる全てのノードについての無効化情報は”００００”以外の値をとることになる。次に鍵設定システム１０４の無効化端末特定部３０３により無効化端末が特定され、鍵情報更新部３０４により鍵情報中の無効化情報が更新された後に、暗号化鍵特定部３０６が、暗号化装置１０１の暗号化鍵群格納部２０３に設定すべき暗号化鍵群を特定するために行う鍵特定処理について説明する。

【００７６】図１３は、暗号化鍵特定部３０６により実行される鍵特定処理を示すフローチャートである。まず、暗号化鍵特定部３０６は、４分木の木構造における最上位層のノード、即ちルートに着目する（ステップＳ３１）。続いて暗号化鍵特定部３０６は、着目しているノード（着目ノード）について、鍵情報格納部３０１に格納されている鍵情報を参照して、その着目ノードの無効化情報に合致する無効化パターンが存在するかを判定し（ステップＳ３２）、もし無効化パターンが存在する場合にはその着目ノードについてのその無効化パターンに対応する暗号化鍵を、暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目ノードの１層下の層が木構造における最下位層でないと判定した場合に限り（ステップＳ３４）、着目ノードの子ノードのうちに無効ノードが存在すればその全ての無効ノードを着目予定ノードと定める（ステップＳ３５）。

【００７７】ステップＳ３２において、無効化情報に合致する無効化パターンが存在しないと判定した場合には、暗号化鍵特定部３０６は、着目ノードの子ノードの属する層は木構造における最下位層か否かを判定し（ステップＳ３６）、着目ノードの子ノードの属する層が最下位層であれば着目ノードの子ノードのうち無効化端末に対応するリーフ以外のものに割り当てられている暗号化鍵を、暗号化装置１０１に設定すべき暗号化鍵として特定する（ステップＳ３７）。

【００７８】ステップＳ３６において、着目ノードの子ノードの属する層が最下位層でないと判定した場合には、暗号化鍵特定部３０６は、着目ノードの全ての子ノードを着目予定ノードと定める（ステップＳ３８）。ステップＳ３５、Ｓ３７、Ｓ３８の後、或いはステップＳ３４において着目ノードの１層下の層が最下位層であると判定した後に、暗号化鍵特定部３０６は、未だ着目していない着目予定ノードが存在するか否かを判定し（ステップＳ３９）、未だ着目していない着目予定ノードが存在する場合には未着目の着目予定ノードのうちの１つのノードに新たに着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻る。

【００７９】また、ステップＳ３９において、未だ着目していない着目予定ノードが存在しないと判定した場合には、暗号化鍵特定部３０６は、鍵特定処理を終える。この結果、ステップＳ３３又はＳ３７により特定された全ての暗号化鍵が、鍵特定情報とともに暗号化鍵特定部３０６から出力され、暗号化装置１０１の暗号化鍵群格納部２０３に格納されることになる。

【００８０】図１４は、６４台しか復号装置がないと仮定した場合において、無効化端末がない状態での暗号化鍵等を示す図である。この場合において、暗号化装置１０１の暗号化鍵群格納部２０３に格納される暗号化鍵であって、コンテンツの光ディスク１０２への記録に際してコンテンツ鍵の暗号化に用いられることとなる暗号化鍵は、暗号化鍵０－１Ｋ０００００、つまり０－１Ｋ０００００で表される復号鍵に呼応する１つの暗号化鍵となる。

【００８１】図１５は、６４台しか復号装置がないと仮定した場合において、端末１が無効化端末である状態での暗号化鍵等を示す図である。端末１のみが無効化端末であると、上述した無効化情報更新処理の結果として、鍵情報格納部３０１に格納されている鍵情報については、レベル２の層の相対番号１番のノード１１０３の無効化情報が”１０００”となり、レベル１の層の相対番号１番のノード１１０２の無効化情報が”１０００”となり、レベル０の層のルート１１０１の無効化情報が”１０００”となる。

【００８２】このことを前提として、以下、図１５の例に基づいて、上述した鍵特定処理（図１３参照）の具体的処理内容を説明する。まず、暗号化鍵特定部３０６は、最上位層のノード、即ちルート１１０１に着目する（ステップＳ３１）。続いて暗号化鍵特定部３０６は、着目しているノード（着目ノード）について、鍵情報格納部３０１に格納されている鍵情報を参照して、そのノード１１０１の無効化情報である”１０００”は、上述した１１種類の無効化パターンの１つと合致するので（ステップＳ３２）、その無効化パターンに対応する暗号化鍵０－１Ｋ１０００を、暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目ノードの１層下の層はレベル１の層であり最下位層ではないため（ステップＳ３４）、着目ノードの子ノードのうちに存在する無効ノードであるノード１１０２を着目予定ノードと定める（ステップＳ３５）。

【００８３】ステップＳ３５の後、暗号化鍵特定部３０６は、未だ着目していない着目予定ノードとしてノード１１０２が存在するので（ステップＳ３９）、ノード１１０２を新たに着目ノードとして（ステップＳ４０）、ステップＳ３２の判定処理に戻る。続いて暗号化鍵特定部３０６は、着目ノードについて、鍵情報格納部３０１に格納されている鍵情報を参照して、そのノード１１０２の無効化情報である”１０００”は、上述した１１種類の無効化パターンの１つと合致するので（ステップＳ３２）、その無効化パターンに対応する暗号化鍵１－１Ｋ１０００を、暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目ノードの１層下の層はレベル２の層であり最下位層ではないため（ステップＳ３４）、着目ノードの子ノードのうちに存在する無効ノードであるノード１１０３を着目予定ノードと定める（ステップＳ３５）。

【００８４】ステップＳ３５の後、暗号化鍵特定部３０６は、未だ着目していない着目予定ノードとしてノード１１０３が存在するので（ステップＳ３９）、ノード１１０３を新たに着目ノードとして（ステップＳ４０）、ステップＳ３２の判定処理に戻る。続いて暗号化鍵特定部３０６は、着目ノードについて、鍵情報格納部３０１に格納されている鍵情報を参照して、そのノード１１０３の無効化情報である”１０００”は、上述した１１種類の無効化パターンの１つと合致するので（ステップＳ３２）、その無効化パターンに対応する暗号化鍵２－１Ｋ１０００を、暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目ノードの１層下の層はレベル３の層であり最下位層であるため（ステップＳ３４）、ステップＳ３５をスキップし、未だ着目していない着目予定ノードはもう存在しないので（ステップＳ３９）、鍵特定処理を終える。

【００８５】この鍵特定処理の結果として、暗号化装置１０１の暗号化鍵群格納部２０３に格納される暗号化鍵群であって、コンテンツの光ディスク１０２への記録に際してコンテンツ鍵の暗号化に用いられることとなる暗号化鍵群は、それぞれ暗号化鍵０－１Ｋ１０００、１－

１Ｋ１０００、２－１Ｋ１０００となる。なお、暗号化鍵特定部３０６は、上述の鍵特定処理により特定した暗号化鍵それぞれに対応する、鍵情報５００（図９参照）中のノードＩＤ、無効化パターン等から、鍵特定情報を作成して出力し、この鍵特定情報は暗号化装置１０１の暗号化鍵群格納部２０３に格納され、暗号化装置１０１によりコンテンツ等とともに光ディスク１０２に記録されることになる。

【００８６】図１６は、図１５に示す暗号化鍵に対応する鍵特定情報の一例を示す図である。同図の例は、鍵情報５００中のノードＩＤである文字列と「Ｋ」という文字と無効化パターンの文字列とを結合して、鍵特定情報を構成した例である。なお、暗号化装置１０１の出力部２０６は、図１６に示した鍵特定情報を光ディスクに記録する場合には、光ディスクには暗号化鍵０－１Ｋ１０００を用いた暗号化により生成された暗号化コンテンツ鍵と、暗号化鍵１－１Ｋ１０００を用いた暗号化により生成された暗号化コンテンツ鍵と、暗号化鍵２－１Ｋ１０００を用いた暗号化により生成された暗号化コンテンツ鍵とをこの順序が識別できるような方法で記録する。

【００８７】＜暗号化コンテンツの復号＞以下、図１５に示す各暗号化鍵を用いた暗号化により生成された各暗号化コンテンツ鍵と暗号化コンテンツと図１６に示す鍵特定情報とが記録された光ディスク１０２から、１台の復号装置１０３ｎがコンテンツを復号して再生する具体的手順について説明する。なお、復号装置１０３ｎは、復号装置１０３ａと同様の構成を備え、復号鍵群格納部２１２の内容のみが異なるので、ここでは復号装置１０３ｎの各部を図２中の符号を用いて説明する。

【００８８】復号装置１０３ｎの復号鍵選定部２１３は、取得部２１１を介して光ディスク１０２から鍵特定情報を読み出し、復号鍵群格納部２１２内に保持している各復号鍵とノードとの対応を示す情報、例えば、鍵情報５００中の各復号鍵に対応するノードＩＤ及び無効化パターンなる情報と、その鍵特定情報とを照合することにより、鍵特定情報で特定される暗号化鍵と、同一のノードについての同一の無効化パターンに対応する復号鍵、即ちその暗号化鍵に呼応する復号鍵を選定し、その復号鍵を復号鍵群格納部２１２中から取り出して鍵復号部２１４に与える。これを受けて、鍵復号部２１４は、取得部２１１を介して取得されたその暗号化鍵で暗号化された暗号化コンテンツ鍵を、その復号鍵を用いて復号する。このような手順により、例えば、復号装置１０３ｎの復号鍵群格納部２１２内に復号鍵０－１Ｋ１０００が含まれていれば、復号装置１０３ｎは、図１６に示す鍵特定情報が記録された光ディスク１０２中における、暗号化鍵０－１Ｋ１０００を用いて暗号化されたコンテンツ鍵を、その復号鍵０－１Ｋ１０００を用いて復号しコンテンツ鍵を得ることになる。

【００８９】コンテンツ鍵を得た後には、復号装置１０３ｎは、コンテンツ復号部２１５において、そのコンテンツ鍵を用いて、取得部２１１を介して取得された暗号化コンテンツを復号してコンテンツを得て、再生部２１６においてそのコンテンツを再生する。なお、図１５における端末１が復号装置１０３ａであるとした場合に、復号装置１０３ａは、図１１に示される２２個の復号鍵しか保持しておらず、０－１Ｋ１０００、１－１Ｋ１０００及び２－１Ｋ１０００のいずれの復号鍵も保持していないため、図１５に示す各暗号化鍵を用いた暗号化により生成され光ディスク１０２に記録された各暗号化コンテンツ鍵を正しく復号することができず、このため光ディスク１０２に記録されている暗号化コンテンツを正しく復号することができず、コンテンツの再生が行えない。

【００９０】＜考察＞データ保護システム１００では、復号装置の数を約１０億台（≒4^{15}台）とした場合には、レベル０からレベル１５までの階層からなる４分木の木構造が構築される必要がある。この場合に、１台の復号装置を無効化端末としたとすれば、暗号化鍵特定部３０６による鍵特定処理において、その１台の無効化端末に対応するリーフからルートに至る経路上に存在する、リーフを除く全１５個の各ノードについての１つの無効化パターンに対応する暗号化鍵が特定されることになり、この結果として、暗号化装置１０１においてコンテンツ鍵を暗号化するために１５個の暗号化鍵が用いられることになる。このとき、光ディスク１０２には、暗号化コンテンツと１５個の暗号化コンテンツ鍵と鍵特定情報とが記録されることになる。

【００９１】また、例えば、この約１０億台の復号装置中の約１万６０００台（≒4^7台）の復号装置を無効化端末としたとすれば、暗号化装置１０１においてコンテンツ鍵を暗号化するために、約１３万１０７２個（4^7×（１５－７）個）の暗号化鍵が用いられることとなる。このとき、光ディスク１０２には、暗号化コンテンツと約１３万１０７２個の暗号化コンテンツ鍵と鍵特定情報とが記録されることになる。

【００９２】１個の暗号化コンテンツ鍵を６４ビット、即ち８バイト（Ｂｙｔｅ）とすれば、約１３万１０７２個分の暗号化コンテンツ鍵は、全部で約１メガバイト（ＭＢ）となる。従って、暗号化コンテンツ鍵の全データ量は、一般的な光ディスクの容量に対して十分に小さいデータ量であると言える。以下、本実施の形態以外の方法を用いて暗号化を行った場合における暗号化コンテンツ鍵の全データ量について検討する。

（１）暗号化コンテンツ鍵が８バイトであり、復号装置の数を約１０億台として約１万６０００台の復号装置を無効化端末とするという前提の下で、仮に全ての復号装置が異なる１つの復号鍵を保持させておいて、無効化端末以外の全ての復号装置それぞれが保持している復号鍵に呼応する各暗号化鍵を用いてコンテンツ鍵を暗号化し

て光ディスクに記録して配布する方式を採用したならば、光ディスクに記録すべき暗号化コンテンツ鍵の総数は約９億９９９８万４０００個となり、その暗号化コンテンツの全データ量は約７６００メガバイトという大きなものとなってしまい、実用的でない。

（２）同じ前提の下で、仮に、各復号装置にリーフを対応させた４分木の木構造における各ノードに１つの復号鍵のみを割り当てておき、各復号装置には、その復号装置に対応するリーフとそのリーフから上層に向けて辿ると到達できる全てのノードとのそれぞれに割り当てられている復号鍵を保持させておいて、無効化端末に対応する１つのリーフから上層に向けて辿ると到達できる全てのノード（つまり無効ノード）についての全ての子ノードのうち無効ノードでないノードそれぞれに割り当てられている暗号化鍵を用いてコンテンツ鍵を暗号化して光ディスクに記録して配布する方式を採用したならば、木構造の最下位層のレベルは１５となり、光ディスクに記録すべき暗号化コンテンツ鍵の総数は約３９万３２１６個（4^7×（１５－７）×３個）となり、その暗号化コンテンツの全データ量は約３メガバイトとなり、本実施の形態に係るデータ保護システム１００による場合よりも、データ量がかなり多くなる。

（３）同じ前提の下で、仮に、各復号装置にリーフを対応させた２分木の木構造における各ノードに１つの復号鍵のみを割り当てておき、各復号装置には、その復号装置に対応するリーフとそのリーフから上層に向けて辿ると到達できる全てのノードとのそれぞれに割り当てられている復号鍵を保持させておいて、無効化端末に対応する１つのリーフから上層に向けて辿ると到達できる全てのノード（つまり無効ノード）についての全ての子ノードのうち無効ノードでないノードそれぞれに割り当てられている暗号化鍵を用いてコンテンツ鍵を暗号化して光ディスクに記録して配布する方式を採用したならば、木構造の最下位層のレベルは３０となり光ディスクに記録すべき暗号化コンテンツ鍵の総数は約２６万２１４４個（2^{14}×（３０－１４）個）となり、その暗号化コンテンツの全データ量は約２メガバイトとなり、本実施の形態に係るデータ保護システム１００による場合よりも、データ量がかなり多くなる。

＜実施の形態２＞以下、本発明の実施の形態２に係るデータ保護システム（以下、「第２データ保護システム」という。）について図を用いて説明する。

【００９３】第２データ保護システムでは、復号鍵及び暗号化鍵の決定に用いるための木構造を複数個用いている点が、データ保護システム１００と異なる点である。第２データ保護システムは、実施の形態１で示したデータ保護システム１００と基本的に同じ構成要素（図１～図３参照）を備える。従って、ここでは第２データ保護システムの構成要素についても図１～図３に示した符号を用いて説明する。なお、ここでは、第２データ保護システムについて、データ保護システム１００と異なる点を中心に説明し、同様である点についての説明は省略する。

【００９４】第２データ保護システムにおける鍵情報生成部３０２、鍵情報更新部３０４、復号鍵決定部３０５及び暗号化鍵特定部３０６の具体的動作内容はデータ保護システム１００中の対応する各部と異なるが、各部の行う基本となる処理内容（図１０、図１２、図１３に示した手順等）は、ほとんど同じであり、第２データ保護システムにおける鍵情報格納部３０１には最下位層以外の各ノードに、実施の形態１において図９で示した１１種類の無効化パターンとともに１１組の復号鍵及び暗号化鍵が対応付けられ、最下位層の各ノードには１組の復号鍵及び暗号化鍵が対応付けられて記憶されている。

【００９５】第２データ保護システムにおける鍵設定システム１０４においては、鍵情報生成部３０２により、図１７に示すような、４分木の木構造を４つ構築し、４つの木構造における全リーフのそれぞれを、復号装置１０３ａ～１０３ｎそれぞれと対応させる。従って、４つのルート１３０１～１３０４が存在し、各復号装置はいずれかの木構造のリーフに対応する。

【００９６】図１７は、実施の形態２に係る第２データ保護システムにおいて復号装置数が６４台である場合に構築される４つの４分木の木構造の例を示す図である。この場合において、リーフが６４個存在するように４つの４分木の木構造が構築されるため、最下位層はレベル２となる。例えば、第２データ保護システムにおける復号鍵決定部３０５の鍵割当処理により（図１０参照）、図１７に示した端末１に割り当てられ、最終的に端末１に保持されることになる復号鍵群は、レベル２の相対番号１のリーフに割り当てられている復号鍵２－１Ｋと、そのリーフの親ノードであるレベル１の相対番号１のノードについて割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する復号鍵、即ち”０００”、”０００１”、”００１０”、”００１１”、”０１００”、”０１０１”及び”０１１０”という７つの無効化パターンに対応する７つの復号鍵１－１Ｋ０００、１－１Ｋ０００１、１－１Ｋ００１０、１－１Ｋ００１１、１－１Ｋ０１００、１－１Ｋ０１０１及び１－１Ｋ０１１０と、そのさらに１層上の親ノードであるレベル０の相対番号１のノード即ちルート１３０１について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する７つの復号鍵０－１Ｋ０００、０－１Ｋ０００１、０－１Ｋ００１０、０－１Ｋ００１１、０－１Ｋ０１００、０－１Ｋ０１０１及び０－１Ｋ０１１０との合計１５個の復号鍵である。

【００９７】また例えば、第２データ保護システムにおける復号鍵決定部３０５により、図１７に示した端末１

７に割り当てられ、端末１７に保持されることになる復号鍵は、レベル２の相対番号１７のリーフに割り当てられている復号鍵２－１７Ｋと、そのリーフの親ノードであるレベル１の相対番号５のノードについて割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する復号鍵、即ち”００００”、”０００１”、”００１０”、”００１１”、”０１００”、”０１０１”及び”０１１０”という７つの無効化パターンに対応する７つの復号鍵１－５Ｋ００００、１－５Ｋ０００１、１－５Ｋ００１０、１－５Ｋ００１１、１－５Ｋ０１００、１－５Ｋ０１０１及び１－５Ｋ０１１０と、そのさらに１層上の親ノードであるレベル０の相対番号１のノード即ちルート１３０２について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する７つの復号鍵０－２Ｋ００００、０－２Ｋ０００１、０－２Ｋ００１０、０－２Ｋ００１１、０－２Ｋ０１００、０－２Ｋ０１０１及び０－２Ｋ０１１０との合計１５個の復号鍵である。

【００９８】また、図１７に示すように、無効化端末がない状態において第２データ保護システムにおける暗号化鍵特定部３０６により特定され（図１３参照）、暗号化装置１０１に設定され光ディスク１０２へコンテンツ鍵を暗号化して記録する際に用いられる暗号化鍵は、暗号化鍵０－１Ｋ００００、０－２Ｋ００００、０－３Ｋ００００及び０－４Ｋ００００なる４つの鍵となる。

【００９９】図１８は、第２データ保護システムにおいて、端末１が無効化端末である状態での暗号化鍵等を示す図である。端末１のみが無効化端末であると、無効化情報更新処理（図１２参照）の結果として、鍵情報格納部３０１に格納されている鍵情報は、レベル１の層の相対番号１番のノード１４０５の無効化情報が”１０００”となり、レベル０の層のルート１４０１の無効化情報が”１０００”となり、暗号化鍵特定部３０６により実行される鍵特定処理（図１３参照）によって、暗号化装置１０１に設定されるべきものとして特定される暗号化鍵は、暗号化鍵０－１Ｋ１０００、１－１Ｋ１０００、０－２Ｋ００００、０－３Ｋ００００及び０－４Ｋ００００なる５つの鍵となる。

【０１００】なお、第２データ保護システムにおける暗号化装置１０１及び復号装置１０３ａ～１０３ｎの動作は、実施の形態１に示したデータ保護システム１００における該当装置の動作と同様である。

＜実施の形態３＞以下、本発明の実施の形態３に係るデータ保護システム（以下、「第３データ保護システム」という。）について図を用いて説明する。

【０１０１】第３データ保護システムは、実施の形態１及び２で示した無効化パターンとは異なる内容の無効化パターンを用いる点に特徴があるが、その他の点は基本的にデータ保護システム１００と変わりない。第３データ保護システムは、実施の形態１で示したデータ保護システム１００と基本的に同じ構成要素（図１～図３参照）を備える。従って、ここでは第３データ保護システムの構成要素についても図１～図３に示した符号を用いて説明する。なお、ここでは、第３データ保護システムについて、データ保護システム１００と異なる点を中心に説明し、同様である点についての説明は省略する。

【０１０２】第３データ保護システムにおける鍵情報格納部３０１には、最下位層以外の各ノードについて、無効化パターンとともに５組の復号鍵及び暗号化鍵が対応付けられ、最下位層の各ノードには１組の復号鍵及び暗号化鍵が対応付けられて記憶されている。但し、実施の形態１及び２においては、あるノードについての無効化情報のとり得る”００００”、”１０００”等の値のうち、”１”の数がｎ分木の木構造である場合における（ｎ－１）個未満となる値を無効化パターンと称することとしたが、実施の形態３における無効化パターンとは、あるノードについての無効化情報のとり得る値のうち、”１”の数が２個未満となる各値をいうこととする。

【０１０３】従って、無効化パターンは、”００００”、”０００１”、”００１０”、”０１００”及び”１０００”の５種類存在し、鍵情報生成部３０２により、リーフ以外の各ノードには、全無効化パターン分の５組の暗号化鍵及び復号鍵が対応付けられ、リーフには１組の暗号化鍵及び復号鍵が対応付けられてなる鍵情報が生成され、鍵情報格納部３０１に格納される。

【０１０４】図１９は、実施の形態３において用いられる４分木の木構造における各ノードに割り当てられている復号鍵を示す図である。同図に示すように、例えばルートには０－１Ｋ００００、０－１Ｋ０００１、０－１Ｋ００１０、０－１Ｋ０１００及び０－１Ｋ１０００の５つの復号鍵が割り当てられており、レベル１の相対番号１のノードには、１－１Ｋ００００、１－１Ｋ０００１、１－１Ｋ００１０、１－１Ｋ０１００及び１－１Ｋ１０００の５つの復号鍵が割り当てられている。

【０１０５】以下、６４台しか復号装置がない場合を例にして、第３データ保護システムの動作について説明する。図２０は、６４台しか復号装置がないと仮定した場合においてレベル３の相対番号１のリーフに対応する復号装置（端末１）に割り当てられる復号鍵群１７０５を示す図である。

【０１０６】第３データ保護システムにおける復号鍵決定部３０５の鍵割当処理（図１０参照）により、図２０に示した端末１に割り当てられ、最終的に端末１に保持されることになる復号鍵群１７０５は、レベル３の相対番号１のリーフ１７０４に割り当てられている復号鍵３－１Ｋと、そのリーフの親ノードであるレベル２の相対番号１のノード１７０３について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないこと

を示す無効化パターンに対応する復号鍵、即ち”００００”、”０００１”、”００１０”及び”０１００”という４つの無効化パターンに対応する４つの復号鍵２－１Ｋ０００、２－１Ｋ０００１、２－１Ｋ００１０及び２－１Ｋ０１００と、その１層上の親ノードであるレベル１の相対番号１のノード１７０２について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する４つの復号鍵１－１Ｋ０００、１－１Ｋ０００１、１－１Ｋ００１０及び１－１Ｋ０１００と、そのさらに１層上の親ノードであるレベル０の相対番号１のノード即ちルート１７０１について割り当てられている復号鍵のうち、１番目の子ノードが無効ノードでないことを示す無効化パターンに対応する４つの復号鍵０－１Ｋ０００、０－１Ｋ０００１、０－１Ｋ００１０及び０－１Ｋ０１００との合計１３個の復号鍵である。従って、第３データ保護システムによれば実施の形態１で示したデータ保護システム１００においてより各端末が保持する復号鍵の数は少なくて済む。

【０１０７】なお、復号鍵決定部３０５により各端末に割り当てられた復号鍵群は、各端末の製造工程等において各端末の復号鍵群格納部２１２に格納される。以下、第３データ保護システムの運用段階において光ディスク１０２へのコンテンツ等の記録に際して必要とされる暗号化鍵について説明する。６４台しか復号装置がないと仮定した場合において、無効化端末がない状態では、第３データ保護システムにおける暗号化鍵特定部３０６の鍵特定処理により特定され、暗号化装置１０１の暗号化鍵群格納部２０３に格納され、コンテンツの光ディスク１０２への記録に際してコンテンツ鍵の暗号化に用いられることとなる暗号化鍵は、暗号化鍵０－１Ｋ００００、つまり復号鍵０－１Ｋ００００に呼応する１つの暗号化鍵となる。

【０１０８】図２１は、６４台しか復号装置がないと仮定した場合において、端末１、端末２及び端末１７が無効化端末である状態での暗号化鍵等を示す図である。第３データ保護システムにおける鍵情報更新部３０４の無効化情報更新処理により（図１２参照）、鍵情報格納部３０１内の鍵情報が更新される。なお、無効化情報更新処理は、実施の形態１で示したデータ保護システム１００の鍵情報更新部３０４により行われる内容と全く同一である。この結果、鍵情報格納部３０１に格納されている鍵情報については、レベル３の層の相対番号１番、２番及び１７番のリーフについての無効化情報が”１１１１”となり、レベル２の層の相対番号１番のノード１８０６の無効化情報が”１１００”となり、レベル２の層の相対番号５番のノード１８０７の無効化情報が”１０００”となり、レベル１の層の相対番号１番のノード１８０２の無効化情報が”１０００”となり、レベル１の層の相対番号２番のノード１８０３の無効化情報が”０００”となり、レベル０の層のルート１８０１の無効化情報が”１１００”となり、他のノードの無効化情報は”０００”となる。なお、対応する無効化情報が”０００”のノードが有効ノードであり、それ以外のノードが、無効ノードである。

【０１０９】無効化情報更新処理に続いて暗号化鍵特定部３０６の鍵特定処理（図１３参照）により暗号化鍵の特定が行われる。以下、図２１に示す例に基づく鍵特定処理の具体的処理内容を図１３を用いて説明する。この例においては、最下位層はレベル３となる。

【０１１０】まず、暗号化鍵特定部３０６は、最上位層のノード、即ちルート１８０１に着目する（ステップＳ３１）。続いて暗号化鍵特定部３０６は、着目しているノード１８０１について、鍵情報格納部３０１に格納されている鍵情報を参照して、そのノード１８０１の無効化情報である”１１００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、いずれとも合致しないので、次に着目しているノード１８０１の１層だけ下の層は最下位層であるかを判定し（ステップＳ３６）、着目しているノード１８０１の１層だけ下の層はレベル１の層であり最下位層ではないため、ノード１８０１の全ての子ノードを着目予定ノードと定める（ステップＳ３８）。

【０１１１】このステップＳ３８により、ノード１８０２～１８０５が着目予定ノードとなる。続いて、暗号化鍵特定部３０６は、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定が存在するのでその１つであるノード１８０２に着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻って、鍵情報を参照して、着目しているノード１８０２の無効化情報である”１０００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、合致するのでノード１８０２についての無効化パターン”１０００”に対応する暗号化鍵１－１Ｋ１０００を暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目しているノード１８０２の１層下の層はレベル２の層であり最下位層ではないため（ステップＳ３４）、ノード１８０２の子ノードのうち無効ノードであるノード１８０６を着目予定ノードと定める（ステップＳ３５）。

【０１１２】ステップＳ３５の後、暗号化鍵特定部３０６は、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定が存在するのでその１つであるノード１８０６に着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻る。次に、暗号化鍵特定部３０６は、鍵情報を参照してノード１８０６の無効化情報である”１１００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、いずれとも合致しないので、次に着目しているノード１８０６の１層だけ下の層は最下位層であるかを判

定し（ステップＳ３６）、ノード１８０６の１層だけ下の層はレベル３の層であり最下位層であるため、そのノード１８０６の子ノードのうちの有効ノードであるリーフ１８０８、１８０９それぞれに対応する暗号化鍵３－３Ｋ、暗号化鍵３－４Ｋを暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３７）、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定が存在するのでその１つであるノード１８０３に着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻る。

【０１１３】次に、暗号化鍵特定部３０６は、鍵情報を参照してノード１８０３の無効化情報である”１０００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、合致するのでノード１８０３についての無効化パターン”１０００”に対応する暗号化鍵１－２Ｋ１０００を暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目しているノード１８０３の１層下の層はレベル２の層であり最下位層ではないため（ステップＳ３４）、ノード１８０３の子ノードのうち無効ノードであるノード１８０７を着目予定ノードと定める（ステップＳ３５）。

【０１１４】続いて、暗号化鍵特定部３０６は、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定が存在するのでその１つであるノード１８０７に着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻って、鍵情報を参照して、着目しているノード１８０７の無効化情報である”１０００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、合致するのでノード１８０７についての無効化パターン”１０００”に対応する暗号化鍵２－５Ｋ１０００を暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目しているノード１８０７の１層下の層はレベル３の層であり最下位層であるため（ステップＳ３４）、ステップＳ３５の処理をスキップして、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定が存在するのでその１つであるノード１８０４に着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻る。

【０１１５】次に、暗号化鍵特定部３０６は、鍵情報を参照して、着目しているノード１８０４の無効化情報である”００００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、合致するのでノード１８０４についての無効化パターン”００００”に対応する暗号化鍵１－３Ｋ００００を暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目しているノード１８０４の１層下の層はレベル２の層であり最下位層ではないため（ステップＳ３４）、ノード１８０４の子ノードのうち

無効ノードを着目予定ノードと定めようとする（ステップＳ３５）。しかし、ノード１８０４の子ノードは全て有効ノードなので新たに着目予定ノードは定められない。

【０１１６】続いて、暗号化鍵特定部３０６は、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定ノードであるノード１８０５に着目し（ステップＳ４０）、ステップＳ３２の判定処理に戻り、鍵情報を参照して、着目しているノード１８０５の無効化情報である”００００”が、上述した５種類の無効化パターンのいずれかと合致するかを判定し（ステップＳ３２）、合致するのでノード１８０５についての無効化パターン”００００”に対応する暗号化鍵１－４Ｋ００００を暗号化装置１０１に設定すべき暗号化鍵として特定し（ステップＳ３３）、着目しているノード１８０５の１層下の層はレベル２の層であり最下位層ではないため（ステップＳ３４）、ノード１８０５の子ノードのうち無効ノードを着目予定ノードと定めようとする（ステップＳ３５）。しかし、ノード１８０５の子ノードは全て有効ノードなので新たに着目予定ノードは定められない。

【０１１７】続いて、暗号化鍵特定部３０６は、未着目の着目予定ノードがあるか判定し（ステップＳ３９）、未着目の着目予定ノードはもう存在しないので、鍵特定処理を終える。このような鍵特定処理の結果として、暗号化装置１０１に設定すべきものとして特定された暗号化鍵は、暗号化鍵１－１Ｋ１０００、１－２Ｋ１０００、１－３Ｋ００００、１－４Ｋ００００、２－５Ｋ１０００、３－３Ｋ及び３－４Ｋなる７個の鍵である。

【０１１８】なお、この７個の暗号化鍵は、後に暗号化装置１０１の暗号化鍵群格納部２０３に格納され、鍵暗号化部２０４によりコンテンツ鍵の暗号化に用いられる。また、各暗号化鍵を用いた暗号化により生成された各暗号化コンテンツ鍵が、出力部２０６により、各暗号化鍵に呼応する復号鍵を特定するために用いることのできる鍵特定情報と暗号化コンテンツとともに光ディスク１０２に記録されることになる。

【０１１９】上述の復号鍵決定部３０５による各端末への復号鍵の割当の結果として、この７個の暗号化鍵に呼応する復号鍵はいずれも、端末１、端末２或いは端末７に保持されておらず、また、この７個の暗号化鍵に呼応する復号鍵のうちいずれか１つ以上が、その他の端末には保持されている。従って、この７つの暗号化鍵を用いた暗号化処理によりコンテンツが光ディスク１０２に記録された後においては、端末１、端末２及び端末７から暴露された復号鍵を用いてその光ディスク１０２に記録されたコンテンツの復号処理を正常に行うことはできず、また、他の端末では光ディスク１０２に記録されたコンテンツの復号処理を正常に行うことができるようになる。

＜実施の形態４＞以下、本発明の実施の形態４に係るデータ保護システム（以下、「第４データ保護システム」という。）について図を用いて説明する。

【０１２０】実施の形態１で示したデータ保護システム１００において、暗号化装置１０１が暗号化コンテンツを記録して各復号装置１０３ａ～１０３ｎに配給するための光ディスク１０２は、ＤＶＤ－ＲＯＭ等であることとしたが、第４データ保護システムは、光ディスク１０２を、ＤＶＤ－ＲＯＭ等のいわゆるプレレコーディッドメディアと、ＤＶＤ－ＲＡＭ等のいわゆるレコーダブルメディアとに２分した場合におけるレコーダブルメディアのみを前提とした実施の形態である。

【０１２１】即ち、第４データ保護システムは、レコーダブルメディアである光ディスク１０２に対して、システム側において一定の情報を記録しておき、ユーザが端末により任意のコンテンツをその光ディスク１０２に対して暗号化して記録して、光ディスク１０２を配布することができ、また同一又は別の端末においてユーザが光ディスク１０２に記録されているコンテンツを復号して利用できるようにしたシステムである。なお、ここでは、第４データ保護システムについて、データ保護システム１００と異なる点を中心に説明し、同様である点についての説明は省略する。

【０１２２】図２２は、本発明の実施の形態４に係る第４データ保護システムの概略構成図である。第４データ保護システムは、同図に示すように、鍵特定情報記録装置１５０１、複数のユーザデータ暗号化装置（端末）１５０２ａ～１５０２ｎ、複数の復号装置（端末）１０３ａ～１０３ｎ及び鍵設定システム１０４を備える。例えば、鍵設定システム１０４及び鍵特定情報記録装置１５０１は著作権保護の管理を行う機関に運用され、各端末は一般ユーザに利用されることが想定される。

【０１２３】なお、復号装置１０３ａ～１０３ｎは実施の形態１で示したものと同一であり、また、ユーザデータ暗号化装置１５０２ａ～１５０２ｎの全部又は一部は復号装置１０３ａ～１０３ｎの全部又は一部と同一の端末に実装されることとしてもよい。また、第４データ保護システムにおける鍵設定システム１０４は実施の形態１で示したものと基本的に同一であるが、若干の機能追加がある。即ち、第４データ保護システムにおける鍵設定システム１０４は、予め各端末をリーフに対応させた４分木の木構造の構築を前提として、図１０に示す鍵割当処理により各端末に復号鍵群を割り当てるが、この際に、割当対象の端末が復号装置であれば復号鍵群を割り当て、割当対象の端末がユーザデータ暗号化装置であればその復号鍵群に呼応する暗号化鍵群を割り当てるものとする。なお、鍵設定システム１０４は、各端末に対して割り当てた鍵と木構造におけるノードとの対応を示す情報を生成して出力する。

【０１２４】この実施の形態４においては、便宜上、ユーザデータ暗号化装置１５０２ａ～１５０２ｎがそれぞれ、復号装置１０３ａ～１０３ｎのそれぞれと同一端末に実装されているものとし、また、呼応する暗号化鍵と復号鍵は同一値であることとして説明する。従って、予め各端末には鍵設定システム１０４により割り当てられた復号鍵群でありかつ暗号化鍵群である鍵群と、その各鍵と木構造におけるノードとの対応を示す情報とを鍵設定システム１０４から取得して保持する。

【０１２５】また、第４データ保護システムにおける鍵設定システム１０４は更に、運用段階において無効化情報更新処理（図１２参照）及び鍵特定処理（図１３参照）の結果として特定された１又は複数の暗号化鍵を指し示す鍵特定情報（図１６参照）を、鍵特定情報記録装置１５０１に出力する機能を有する。例えば、無効化端末がない状態では、鍵特定情報は、「０－１Ｋ０００」のみとなる。

【０１２６】鍵特定情報記録装置１５０１は、データを光ディスクに記録可能なハードウェアを含み、鍵設定システム１０４から入力された鍵特定情報を光ディスク１０２に記録する機能を有する装置である。また、ユーザデータ暗号化装置１５０２ａ～１５０２ｎそれぞれは、実施の形態１で示した暗号化装置１０１（図２参照）の各機能に相当する機能を備える。但し、コンテンツ記憶部２０１にはユーザが自由にデジタルコンテンツを格納することができ、暗号化鍵群格納部２０３の内容は、上述した鍵設定システム１０４から取得して端末が保持している暗号化鍵群と、各暗号化鍵と木構造におけるノードとの対応を示す情報とであり、鍵暗号化部２０４が乱数発生部２０２から取得したコンテンツ鍵の暗号化に用いる暗号化鍵は、後述する暗号化鍵選定処理の結果として選定されたものであり、また、出力部２０６は、鍵特定情報を光ディスク１０２に記録せず、暗号化コンテンツ及び暗号化コンテンツ鍵を光ディスク１０２に記録する。

【０１２７】また、ユーザデータ暗号化装置１５０２ａ～１５０２ｎそれぞれは、更に光ディスク１０２から鍵特定情報記録装置１５０１によって記録された鍵特定情報を読み出してコンテンツ鍵の暗号化に用いる暗号化鍵を選定する暗号化鍵選定処理を行う機能を有する。この暗号化鍵選定処理は、暗号化鍵群格納部２０３内の各暗号化鍵とノードとの対応を示す情報と鍵特定情報とを照合して、両者に同じノードを示す内容があればそのノードに対応する暗号化鍵を選定して鍵暗号化部２０４に送出する処理であり、実施の形態１で示した復号装置１０３ａ中の復号鍵選定部２１３における復号鍵を選定する処理と同様の処理である。

【０１２８】即ち、ユーザデータ暗号化装置１５０２ａ～１５０２ｎそれぞれは、光ディスク１０２にコンテンツをコンテンツ鍵で暗号化して記録する場合において、光ディスク１０２内に予め記録されている鍵特定情報に

従った暗号化鍵を用いてコンテンツ鍵を暗号化して光ディスク１０２に記録する機能を有する装置である。従って、この第４データ保護システムによれば、不正に解析される等して復号鍵等が暴露された端末以外の多数の端末において、暴露された復号鍵によっては正しく復号できず、暴露されていない復号鍵を持つ多数の端末では正しく復号して利用できるようにコンテンツを暗号化して光ディスク１０２に記録することができるようになる。

＜補足＞以上、本発明に係るデータ保護システムについて、実施の形態１～４に基づいて説明したが、本発明はこれらの実施の形態に限られないことは勿論である。即ち、

（１）実施の形態１～４で示したコンテンツは映像、音声等であることとしたが、コンテンツの内容はこれらに限定されることはなく、プログラムその他のデータであっても、これらと映像等との組み合わせであってもよい。

（２）実施の形態１～４で示した復号装置は、復号したコンテンツを再生する再生部２１６を備えることとしたが、その代わりに復号したコンテンツを装置外部に出力する機能を有することとしてもよい。

（３）実施の形態１～３では、暗号化コンテンツ等を光ディスク１０２に記録して各復号装置に配布する形態を示したが、暗号化コンテンツ等を各復号装置に配給する形態として、記録媒体による配布の他に、無線又は有線の伝送路を通じて配信するという形態としてもよい。

【０１２９】暗号化コンテンツ等を配信する形態を採用する場合においては、暗号化装置１０１の出力部２０６は、通信機能を有するハードウェアを備えるものとし、暗号化コンテンツ、暗号化コンテンツ鍵及び鍵特定情報を各復号装置（端末）に送信することとする必要があり、復号装置１０３ａ等の取得部２１１は、通信機能を有するハードウェアを備えるものとし、暗号化コンテンツ、暗号化コンテンツ鍵及び鍵特定情報を受信して取得することとする必要がある。なお、配信の方法としては、例えば、暗号化装置１０１が例えばインターネットに接続されているサーバ中の記録媒体に記録し復号装置１０３ａ等がその記録媒体の内容をインターネットを通じて受信することとしてもよい。

【０１３０】また、暗号化コンテンツ等を記録媒体に記録して配布する形態を採用する場合における記録媒体は、光ディスクに限られることはなく、ＩＣカード、フレキシブルディスク、磁気テープ、ＲＯＭ等であってもよい。

（４）実施の形態１で示した鍵情報における各ノードに対応する無効化パターンの定め方は、単なる一例であり、例えばルート以外の各ノードが”００００”という無効化パターンを持たないこととし、リーフ以外の各ノードが”０１１１”、”１１０１”、”１０１１”、”１１１０”という無効化パターンを持つこととして、これに合わせて鍵割当処理（図１０参照）及び鍵特定処理（図１３参照）の内容を若干変更することとしてもよい。

【０１３１】また、実施の形態１等では４分木の木構造の構築を前提として無効化パターン等を定めたが、前提となる木構造は、ｎが３以上であるｎ分木の木構造を少なくとも一部に含む木構造、つまり少なくとも一層における１のノードが３以上の子ノードの親ノードであるような木構造であればよく、３分木であっても、５分木であってもよく、各層において３分木や４分木等が異なるような木構造を用いることとしてもよい。

【０１３２】また、実施の形態１では、４分木の木構造の各ノードについての無効化パターンは「１」の数が３未満のものに限ることとしており、実施の形態３では、４分木の木構造の各ノードについての無効化パターンは「１」の数が２未満のものに限ることとしたが、例えば５分木の木構造の各ノードについての無効化パターンは「１」の数が２未満のものに限ることとしても、３未満のものに限ることとしても、４未満のものに限ることとしてもよい。

（５）実施の形態１～４に示した復号装置１０３ａ～１０３ｎにおける復号に関連する各部及び実施の形態４に示したユーザデータ暗号化装置１５０２ａ～１５０２ｎにおける暗号化に関連する各部は、いわゆる耐タンパ技術により、復号又は暗号化に用いられる方式やデータが保護されるように構成されることが望ましい。

（６）実施の形態１等で鍵設定システムは各端末に割り当てるべき復号鍵を決定した際に復号鍵と、その復号鍵が対応する木構造におけるノードを示す情報とを出力し、この結果として復号装置１０３ａ～１０３ｎが復号鍵群と、各復号鍵に対応するノードを示す情報とを保持することとしたが、復号装置は、必ずしも復号鍵に対応するノードを示す情報を保持する必要はない。復号鍵に対応するノードを示す情報を保持しない場合においては、光ディスクに記録されている暗号化コンテンツ鍵を、復号装置は自ら保持している各復号鍵を順次用いた復号を試みる方法により、コンテンツ鍵を復号することとしてもよい。なお、この場合、コンテンツ鍵には予め先頭８ビットが０である等の規則を設けておくことや、一般的なデジタル署名等を用いて、復号したコンテンツ鍵の正当性が確認できるようにしておくこととし、復号装置は、復号したコンテンツ鍵が正当であるときにのみそのコンテンツ鍵を用いてコンテンツを復号するようにしてもよい。

（７）実施の形態１ではコンテンツ鍵、復号鍵及び暗号化鍵は６４ビットであることとしたが、鍵のデータサイズについては６４ビットに限定されることはなく、他のビット数であってもよい。なお、図１６において、鍵特定情報がノードＩＤである文字列と「Ｋ」という文字と無効化パターンの文字列とを結合してなる文字列を含む

こととしたが、鍵特定情報のフォーマットはこれに限定されることはない。

（８）実施の形態１～４では、コンテンツの暗号化に用いられるコンテンツ鍵を、０－１Ｋ００００等で表される暗号化鍵を用いた暗号化の対象としたが、暗号化の対象は、コンテンツ鍵に限定されることはなく、機密保持を要するいかなるデータであってもよい。

（９）実施の形態１～４に示した鍵設定システム１０４における無効化情報更新処理、鍵割当処理又は鍵特定処理（図１０、図１２又は図１３に示した手順等）をコンピュータ又はプログラム実行機能を備える機器に実行させるためのコンピュータプログラムを、記録媒体に記録し又は各種通信路等を介して、流通させ頒布することもできる。このような記録媒体には、ＩＣカード、光ディスク、フレキシブルディスク、ＲＯＭ等がある。流通、頒布されたコンピュータプログラムはコンピュータ等にインストールされることにより利用に供され、コンピュータ等はそのコンピュータプログラムの実行により実施の形態１～４で示したような無効化情報更新処理、鍵割当処理又は鍵特定処理を行う。

【０１３３】

【発明の効果】以上説明したことから明らかなように、本発明に係るデータ保護システムは、３台以上の端末、暗号化装置及び暗号化鍵特定装置を備え、各端末への配給用データを暗号化装置により暗号化して保護するデータ保護システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶しており、前記暗号化装置から出力された暗号化配給用データ群を取得して、暗号化配給用データを、記憶している復号鍵を用いて復号するものであり、前記所定鍵割当方法は、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c)前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であり、前記暗号化鍵特定装置は、暗号化鍵を特定する装置であり、かつ、１つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記所定鍵割当方法により端末に割当てられた全ての復号鍵のうち無効化端末に割当てられた復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が割り当てられていない最も多くの端末に、割当てられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が割り当てられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを有する装置であり、前記暗号化装置は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成して出力する暗号化手段を有することを特徴とする。

【０１３４】ここで、配給用データは、記録媒体に記録されて配布され、或いは有線又は無線の通信路を通じて配信され、最終的に各端末に到達することが想定されるデータである。端末１、端末２、端末３を想定すれば、上述の所定鍵割当方法により決定される端末集合には、端末１及び端末２の組Ａや、端末１及び端末３の組Ｂや、端末２及び端末３の組Ｃがあり、所定鍵割当方法による割り当て結果を受けて端末１が記憶保持する復号鍵は端末１固有の復号鍵と、組Ａに対応する復号鍵Ａと、組Ｂに対応する復号鍵Ｂとであり、端末２が記憶保持する復号鍵は端末２固有の復号鍵と、組Ａに対応する復号鍵Ａと、組Ｃに対応する復号鍵Ｃとであり、端末３が記憶保持する復号鍵は端末３固有の復号鍵と、組Ｂに対応する復号鍵Ｂと、組Ｃに対応する復号鍵Ｃとである。この例において、端末２が不正に解析等されて端末２が記憶保持する全ての復号鍵が暴露されてしまった場合には端末２を無効化端末、つまり無効化にすべき端末として特定し、前記暗号化鍵特定手段による暗号化鍵の特定を行うと復号鍵Ｂに呼応する暗号化鍵が特定されることになる。

【０１３５】従って、復号鍵Ｂに呼応する暗号化鍵を用いてデータを暗号化して各端末に配給すれば、端末２では正しくそのデータを復号することができず、端末１及び端末３では正しくそのデータを復号することができる。同様の目的を、端末１固有の復号鍵に呼応する暗号化鍵と端末３固有の復号鍵に呼応する暗号化鍵とをそれぞれ用いてデータを暗号化して各端末に配給することもできるが、この方法と比べて前述の復号鍵Ｂに呼応する暗号化鍵を用いる方法は、暗号化に用いる暗号化鍵の数が少なく、その分だけ配給される暗号化データのデータ量が少なくなるという効果を有する。

【０１３６】即ち、本発明によれば、暗号化したデジタルコンテンツの復号に必要な鍵等のデータを暗号化して同一データを複数の端末に配給するデータ保護システムにおいて、配給対象の暗号化データの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにすることが可能となる。

【０１３７】また、前記所定鍵割当方法は更に、前記複数の端末集合を完全に包含する端末集合が存在するように、かつ、同じ１つ以上の端末集合を各々包含する複数

の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、端末集合の前記決定を行う方法であることとしてもよい。

【０１３８】例えば、端末集合Ａ及び端末集合Ｂを包含する端末集合ＡＢには復号鍵ＡＢが、端末集合Ｂ及び端末集合Ｃを包含する端末集合ＢＣには復号鍵ＢＣが対応付けられている場合について言えば、このデータ保護システムにおいては、端末集合Ａに属するが端末集合Ｂにも端末集合Ｃにも属さない端末には、少なくとも復号鍵ＡＢが割り当てられ記憶保持されるが復号鍵ＢＣは割り当てられず記憶保持されず、端末集合Ｂ又は端末集合Ｃに属する端末には少なくとも復号鍵ＢＣが割り当てられる。従って、端末集合Ａに属するが端末集合Ｂにも端末集合Ｃにも属さない端末が不正に解析等された後においても、少なくとも復号鍵ＢＣに呼応する暗号化鍵を用いてデータを暗号化して各端末に配給することにより、端末集合ＢＣに包含される端末群即ち端末集合Ｂに包含される端末群及び端末集合Ｃに包含される端末群が復号鍵ＢＣを用いてデータを正しく復号することができるようになり、少ない暗号化鍵を用いて多くの端末で正しく復号できるようにデータを暗号化することが可能になる。

【０１３９】また、前記所定鍵割当方法は更に、各端末集合が３台以上の端末を要素に含むように、かつ、３つ以上の端末集合を包含する端末集合が存在するように、端末集合の前記決定を行う方法であることとしてもよい。これにより、暗号化済みの同一データを各端末に配給する際において、３台以上の端末に共通な鍵を用いた暗号化が行えるので、各々別個な鍵を用いた場合よりも配給対象のデータ量を削減することができるようになる。

【０１４０】また、前記データ保護システムは、各端末を各々別個の最下位層のノードに対応させた複数階層のＮ分木（Ｎは３以上の自然数）の木構造を想定した場合における最下位層を除く各ノードについて、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなりＮ個全部の組合せを含む複数の組合せパターンを決定し、決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶しており、更に最下位層の各ノードに対応付けて別個の復号鍵を記憶している鍵記憶装置と、前記所定鍵割当方法を実行し、前記各端末に割り当てる復号鍵群を決定する装置であり、かつ、前記各端末について、当該端末に対応する最下位層のノードから最上位層のノードまでの経路上に位置する最下位層でない各ノードについて、当該ノードに対応付けて前記鍵記憶装置により記憶されている復号鍵のうち、当該ノードの１段下位層で当該経路上に位置するノードを含む組合せに係る全ての前記組合せパターンに対応する復号鍵と、当該端末に対応付けて前記鍵記憶装置により記憶されている復号鍵とを、当該端末に割り当てるべきものとして決定する復号鍵決定装置とを備え、前記各端末集合は、前記各組合せパターンと一対一に対応し、対応する組合せパターンにおいて組み合わされた全ノードからから辿り着く最下位層のノードに対応する全ての端末を要素とする集合に相当するものであり、前記暗号化鍵特定手段は、前記木構造を想定した場合において、いずれかの無効化端末に対応する最下位層のノードに辿り着く全てのノードを無効ノードと定め、まず最上位層ノードを処理対象ノードとしておき、未処理の処理対象ノードが存在しなくなるまで暗号化鍵特定処理を繰り返し行い、前記暗号化鍵特定処理は、未処理の１つの処理対象ノードについて、(a) 当該処理対象ノードの１段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在する場合には、当該組合せパターンに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、(b) 当該処理対象ノードの１段下位層において無効ノード以外の全てのノードを含む組合せに係る前記組合せパターンが存在しない場合には、当該１段下位層が最下位層であれば当該１段下位層における無効ノード以外の全てのノードに対応して前記鍵記憶装置により記憶されている復号鍵に呼応する暗号化鍵を特定し、当該１段下位層が最下位層でなければ当該１段下位層における無効ノード以外の全てのノードを新たに処理対象ノードとし、(c) 当該処理対象ノードの１段下位層において無効ノードが存在すれば、当該１段階層が最下位層でない限り全ての無効ノードを新たに処理対象ノードとする処理であることとしてもよい。

【０１４１】このように、木構造におけるノード毎に復号鍵等の情報を対応付けておき、その情報と木構造における各ノードの位置付けに基づいて各端末に割り当てる復号鍵を決定し、配給用データの暗号化に用いる暗号化鍵を特定する方式によって、比較的容易に上述の目的、即ち配給対象の暗号化データの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにするという目的を達成するシステムが実現できる。

【０１４２】また、前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、２以上を組合せてなる全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることとしても

よい。

【０１４３】これにより、各端末への配給用データの暗号化に用いる暗号化鍵の特定をｎ分木の木構造を用いて行う方式の中では、特定される暗号化鍵の数が少なく抑えられるので、結果的に各端末へ配給される暗号化配給用データのデータ量を比較的小さく抑えることが可能になる。また、前記鍵記憶装置による、前記木構造を想定した場合における最下位層を除く各ノードについての前記複数の組合せパターンの決定は、当該ノード（親ノード）から辿り着く１段下位層のＮ個のノードのうち、Ｎ個全部の組合せ及び（Ｎ－１）個の全ての組合せそれぞれに対応するように組合せパターンを定めることによりなされ、当該鍵記憶装置は、その決定した組合せパターン毎に別個の復号鍵を定めてその定めた各復号鍵を当該ノード（親ノード）と対応付けて記憶していることとしてもよい。

【０１４４】これにより、各端末への配給用データの暗号化に用いる暗号化鍵の特定をｎ分木の木構造を用いて行う方式の中では、各端末に割り当てられる復号鍵の数が比較的少なく抑えられるので、結果的に各端末が記憶保持する復号鍵群のデータ量を比較的小さく抑えることが可能になる。また、前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵それぞれについて、当該暗号化鍵を用いた暗号化により生成した暗号化配給用データと、前記鍵記憶装置により当該暗号化鍵に呼応する復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための暗号化鍵ノード識別情報とを、対応付けて出力し、前記各端末は、所定鍵割当方法により個別に割当てられた各復号鍵を、前記鍵記憶装置により当該復号鍵と対応付けられていたノードの前記木構造における所在位置を特定するための復号鍵ノード識別情報と対応付けて記憶しており、前記暗号化装置から出力された暗号化配給用データ群及び暗号化鍵ノード識別情報群を取得して、当該端末が記憶している復号鍵ノード識別情報と一致する暗号化鍵ノード識別情報と対応する暗号化配給用データを、当該一致に係る復号鍵ノード識別情報と対応する復号鍵を用いて復号することとしてもよい。

【０１４５】これにより、各端末は、１以上の暗号化鍵をそれぞれ用いて配給用データが暗号化されたものである暗号化配給用データ群を取得した後、暗号化鍵ノード識別情報群を参照することにより、自端末が保持するいずれの復号鍵を用いて復号を行うとよいかを簡単に特定することが可能となり、試行錯誤的に自端末が保持する復号鍵を逐次用いて復号を行う場合に比べて、正しく復号されるまでにかかる時間が短縮される。

【０１４６】また、前記暗号化鍵特定装置は、前記鍵記憶装置により記憶されている各復号鍵に呼応する暗号化鍵を記憶している暗号化鍵記憶手段を有し、前記呼応する復号鍵と暗号化鍵とは互いに異なることとしてもよい。これにより、ある端末の不正な解析等により復号鍵が暴露された場合にも、複数の端末で正しく復号できるようにデータを暗号化するための暗号化鍵が不正に知られて悪用されるような事態の発生を防止することができるようになる。

【０１４７】また、前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群をデータ記録媒体に記録することであり、前記各端末は、前記暗号化装置により暗号化配給用データ群が記録されたデータ記録媒体から当該暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号することとしてもよい。これにより、ＤＶＤ－ＲＯＭ等の光ディスクその他の記録媒体にデータが暗号化して記録されるので、例えばその記録媒体と同一内容の記録媒体を量産して有償又は無償で多数の人に頒布することができ、その頒布された記録媒体を受け取った人はその記録媒体を端末にセットして端末を通じて、その記録媒体に記録されているデータを利用することができるようになる。

【０１４８】また、前記暗号化手段は、デジタル著作物であるコンテンツデータを記憶しているコンテンツ記憶部と、乱数である前記配給用データを生成する乱数データ発生部と、前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツデータを暗号化して、暗号化コンテンツデータを生成するコンテンツ暗号化部とを有し、前記暗号化手段は、前記暗号化鍵特定装置により特定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより、暗号化配給用データ群を生成して、当該暗号化配給用データ群と、前記コンテンツ暗号化部により生成された暗号化コンテンツデータとを前記データ記録媒体に記録し、前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することとしてもよい。

【０１４９】これにより、暗号化した映像、音声等のデジタルコンテンツの復号に必要な鍵を暗号化して、暗号化したデジタルコンテンツやその暗号化した鍵を含むデータを記録媒体に記録するので、例えば、その記録媒体と同一内容の記録媒体が多数の人に頒布され、頒布された記録媒体を受け取った人はその記録媒体を端末にセットして端末を通じて、デジタルコンテンツの再生等を行うことができるようになる。

【０１５０】また、前記データ保護システムは更に、前記暗号化鍵特定装置により特定された暗号化鍵を特定するための暗号化鍵特定情報を、データ記録媒体に記録する暗号化鍵特定情報記録装置を備え、前記各端末は、乱数である前記配給用データを生成する乱数データ発生部と、デジタル著作物であるコンテンツデータを格納しているコンテンツ格納部と、前記データ記録媒体から暗号

化鍵特定情報を読み出し、当該端末に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定部とを有し、前記暗号化手段は、前記暗号化鍵選定部により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生部により生成された配給用データを暗号化することにより暗号化配給用データ群を生成して、前記データ記録媒体に記録するものであり、前記各端末は更に、前記乱数データ発生部により生成された配給用データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化して、暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化部と、前記各端末は、前記データ記録媒体から暗号化コンテンツデータ及び暗号化配給用データ群を読み出して取得して、暗号化配給用データを復号し、復号結果である配給用データを用いて、当該暗号化コンテンツデータを復号することとしてもよい。

【０１５１】これにより、ＤＶＤ－ＲＡＭ等の記録媒体に、端末のユーザが任意の映像、音声等のデジタルコンテンツを記録して頒布することが可能なシステムにおいて、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合に、その特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるようにデジタルコンテンツを暗号化することが可能になる。

【０１５２】また、前記暗号化手段による前記出力は、生成した前記暗号化配給用データ群を前記各端末に送信することであり、前記各端末は、前記暗号化装置により送信された暗号化配給用データ群を受信して取得し、暗号化配給用データを復号することとしてもよい。これにより、配給用データは暗号化され各端末に送信されることになるため、各端末においてはその受信により容易に配給用データを利用することが可能になる。

【０１５３】また、本発明に係る復号鍵決定装置は、暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定装置であって、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当手段とを備えることとしてもよい。

【０１５４】また、本発明に係る復号鍵決定方法は、暗号化されたデータを取得して復号するための３台以上の端末それぞれに、個別に割り当てる復号用の復号鍵群を決定するための復号鍵決定方法であって、前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵及び当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に割り当てるべき復号鍵群として決定する復号鍵群割当ステップとを含むことを特徴とする。

【０１５５】また、本発明に係る復号端末システムは、暗号化されたデータを取得して復号するための３台以上の端末から構成される復号端末システムであって、前記各端末は、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段とを備え、前記所定鍵割当方法は、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 前記各端末に対して、当該端末に対応して定めた復号鍵、及び当該端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【０１５６】また、本発明に係る復号端末は、暗号化されたデータを取得して復号するための復号端末であって、所定鍵割当方法により個別に割当てられた復号鍵群を記憶している復号鍵群記憶手段と、暗号化されたデータを取得する暗号化データ取得手段と、前記暗号化データ取得手段により取得されたデータを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号する復号手段と、前記所定鍵割当方法は、(a) 本端末を含む３台以

上の端末を想定した場合において本端末が、２つ以上の端末を要素に含む集合である複数の端末集合に属するように、更に、本端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 本端末に対応して及び決定した端末集合毎に対応して各々別個の復号鍵を定め、(c) 本端末に対して、本端末に対応して定めた復号鍵、及び本端末を含む全ての端末集合の各々に対応して定めた復号鍵を全て割り当てる方法であることを特徴とする。

【０１５７】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【０１５８】また、前記暗号化データ取得手段は、前記暗号化されたデータをデータ記録媒体から読み出して取得することとしてもよい。これにより、暗号化されたデータをデータ記録媒体に記録してその記録媒体を各端末のユーザに配布することによって各端末のユーザにデータを利用させることが可能になる。

【０１５９】また、前記データ記録媒体には、暗号化鍵を特定するための暗号化鍵特定情報が記録されており、前記端末は更に、乱数である鍵データを生成する乱数データ発生手段と、デジタル著作物であるコンテンツデータを格納しているコンテンツ格納手段と、前記データ記録媒体から暗号化鍵特定情報を読み出し、前記復号鍵群記憶手段に記憶されている復号鍵群に呼応する暗号化鍵群のうち当該暗号化鍵特定情報で特定される暗号化鍵を選定する暗号化鍵選定手段と、前記暗号化鍵選定手段により選定された全ての暗号化鍵を逐次用いて前記乱数データ発生手段により生成された鍵データを暗号化することにより暗号化鍵データ群を生成して、当該暗号化鍵データ群を前記データ記録媒体に記録する鍵データ暗号化手段と、前記乱数データ発生手段により生成された鍵データを鍵として用いて前記コンテンツ格納部に格納されているコンテンツデータを暗号化することにより暗号化コンテンツデータを生成し、当該暗号化コンテンツデータを前記データ記録媒体に記録するコンテンツ暗号化手段とを備え、前記暗号化データ取得手段は、前記データ記録媒体に記録されている暗号化鍵データ及び暗号化コンテンツデータを取得し、前記復号手段は、前記暗号化データ取得手段により取得された前記暗号化鍵データを、前記復号鍵群記憶手段に記憶されている復号鍵を用いて復号することにより鍵データを生成するものであり、前記端末は更に、前記暗号化データ取得手段により取得された前記暗号化コンテンツデータを、前記復号手段により生成された鍵データを用いて復号するコンテンツ復号手段を備えることとしてもよい。

【０１６０】これにより、各端末のユーザは、映像、音声等のデジタルコンテンツを暗号化して記録媒体に記録することができるようになる。また、前記暗号化されたデータは外部の送信装置から送信されるものであり、前記暗号化データ取得手段は、前記暗号化されたデータを受信することにより取得することとしてもよい。

【０１６１】これにより、デジタルコンテンツ等の送信されたデータを各端末においては受信により容易に利用することが可能になる。また、本発明に係る暗号化鍵特定装置は、３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定する暗号化鍵特定装置であって、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵群対応付け手段と、前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵設定手段と、１つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段とを備えることを特徴とする。

【０１６２】また、本発明に係る暗号化装置は、３台以上の各端末への配給用データを暗号化する暗号化装置であって、(a) 前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定し、(b) 端末毎及び決定した端末集合毎について各々別個の復号鍵を対応付ける復号鍵設定手段と、

前記各端末に対して、前記復号鍵設定手段により当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付け手段と、１つ以上の端末を無効化端末として特定する無効化端末特定手段と、前記復号鍵群対応付け手段により端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返したと仮定したときに、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定手段と、前記暗号化鍵特定手段により特定された全ての暗号化鍵を逐次用いて配給用データを暗号化し、暗号化配給用データ群を生成する暗号化手段と、前記暗号化手段により生成された暗号化配給用データ群を外部に出力する出力手段とを備えることを特徴とする。

【０１６３】また、本発明に係る暗号化鍵特定方法は、３台以上の各端末への配給用データの暗号化に用いるべき暗号化鍵を特定するための暗号化鍵特定方法であって、前記各端末が、２つ以上の端末を要素に含む集合である端末集合の少なくとも１つには属するように、更に、同じ１つ以上の端末を各々要素に含む複数の端末集合であって、当該複数の端末集合におけるいずれの一の端末集合も当該複数の端末集合における他の各端末集合の部分集合でないという関係が成立するところの当該複数の端末集合が存在するように、２つ以上の端末集合を決定する端末集合決定ステップと、端末毎及び前記端末集合決定ステップにより決定された端末集合毎について各々別個の復号鍵を対応付ける復号鍵対応付けステップと、前記各端末に対して、前記復号鍵対応付けステップにより当該端末に対応付けられた復号鍵に加えて、当該端末を含む全ての端末集合の各々に対応付けられた復号鍵全てを、当該端末に対応付ける復号鍵群対応付けステップと、１つ以上の端末を無効化端末として特定する無効化端末特定ステップと、前記復号鍵群対応付けステップにより端末に対応付けられた全ての復号鍵のうち無効化端末に対応付けられている復号鍵以外の復号鍵を有効復号鍵と定めた場合において、選定済みの有効復号鍵が対応付けられていない最も多くの端末に対応付けられている有効復号鍵を選定するという手順を、選定済みの有効復号鍵が対応付けられていない端末が存在しなくなるまで繰り返し、結果的に選定済みとなる全ての有効復号鍵それぞれに呼応する暗号化鍵を特定する暗号化鍵特定ステップとを含むことを特徴とする。

【０１６４】これらにより、例えば、各端末へ記録媒体に暗号化された結果のデータを記録して記録媒体を配布する場合において、暗号化に用いる暗号化鍵の数を比較的少なく抑えることができるので、その記録媒体に記録されるデータの量の増大化を抑制した上で、特定の端末の解析等によりその端末が保持していた復号鍵が不正者によって暴露された場合にその特定の端末ではデータを正しく復号できず他の端末ではデータを正しく復号できるように、その暗号化を実施することが可能になる。

【図面の簡単な説明】

【図１】本発明の実施の形態１に係るデータ保護システム１００の概略構成図である。

【図２】暗号化装置１０１及び復号装置１０３ａの機能構成図である。

【図３】鍵設定システム１０４の機能構成図である。

【図４】４分木の木構造を示す図である。

【図５】復号装置数が６４台である場合における４分木の木構造の例を示す図である。

【図６】ルートの無効化情報の例を示す図である。

【図７】ルートの無効化情報の例を示す図である。

【図８】４分木の木構造のレベル０及びレベル１の階層のノードに対応して割り当てられる鍵を示す図である。

【図９】鍵情報格納部３０１に格納される鍵情報の構成を示す図である。

【図１０】復号鍵決定部３０５により実行される鍵割当処理を示すフローチャートである。

【図１１】６４台しか復号装置がないと仮定した場合においてレベル３の相対番号１のリーフに対応する復号装置（端末１）に割り当てられるものと鍵割当処理によって決定される復号鍵群９０５を示す図である。

【図１２】鍵情報更新部３０４により実行される無効化情報更新処理を示すフローチャートである。

【図１３】暗号化鍵特定部３０６により実行される鍵特定処理を示すフローチャートである。

【図１４】６４台しか復号装置がないと仮定した場合において、無効化端末がない状態での暗号化鍵等を示す図である。

【図１５】６４台しか復号装置がないと仮定した場合において、端末１が無効化端末である状態での暗号化鍵等を示す図である。

【図１６】図１５に示す暗号化鍵に対応する鍵特定情報の一例を示す図である。

【図１７】実施の形態２に係る第２データ保護システムにおいて復号装置数が６４台である場合に構築される４つの４分木の木構造の例を示す図である。

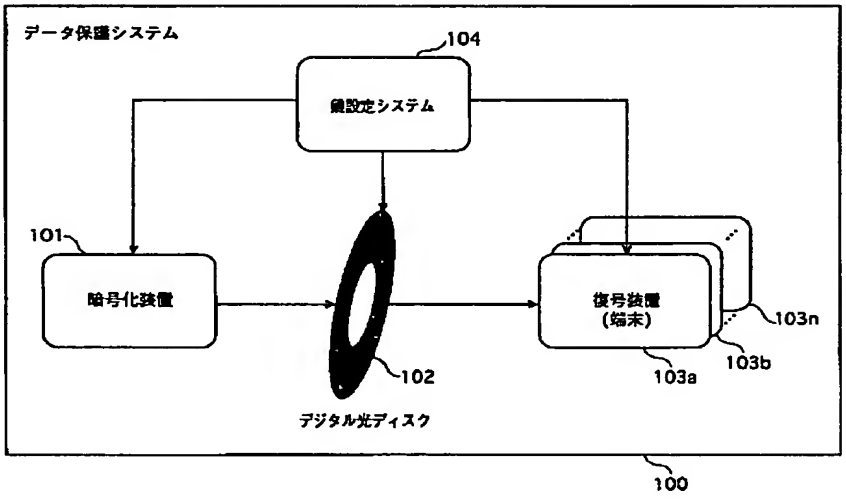
【図１８】第２データ保護システムにおいて、端末１が無効化端末である状態での暗号化鍵等を示す図である。

【図１９】実施の形態３において用いられる４分木の木構造における各ノードに割り当てられている復号鍵を示す図である。

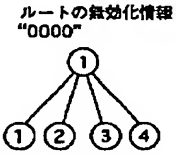
【図２０】６４台しか復号装置がないと仮定した場合においてレベル３の相対番号１のリーフに対応する復号装置（端末１）に割り当てられる復号鍵群１７０５を示す

図である。
【図２１】６４台しか復号装置がないと仮定した場合において、端末１、端末２及び端末１７が無効化端末である状態での暗号化鍵等を示す図である。
【図２２】本発明の実施の形態４に係る第４データ保護システムの概略構成図である。
【符号の説明】
１００　データ保護システム
１０１　暗号化装置
１０２　光ディスク
１０３ａ～１０３ｎ　復号装置
１０４　鍵設定システム
２０１　コンテンツ記憶部
２０２　乱数発生部
２０３　暗号化鍵群格納部
２０４　鍵暗号化部
＊２０５　コンテンツ暗号化部
２０６　出力部
２１１　取得部
２１２　復号鍵群格納部
２１３　復号鍵選定部
２１４　鍵復号部
２１５　コンテンツ復号部
２１６　再生部
３０１　鍵情報格納部
３０２　鍵情報生成部
３０３　無効化端末特定部
３０４　鍵情報更新部
３０５　復号鍵決定部
３０６　暗号化鍵特定部
１５０１　鍵特定情報記録装置
＊　１５０２ａ～１５０２ｎ　ユーザデータ暗号化装置

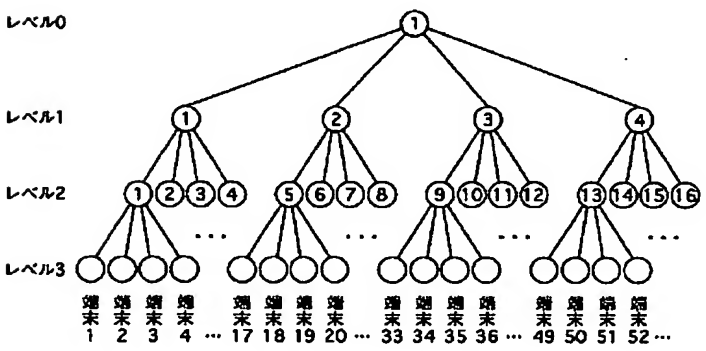
【図１】



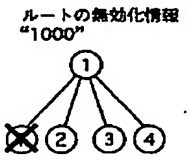
【図６】



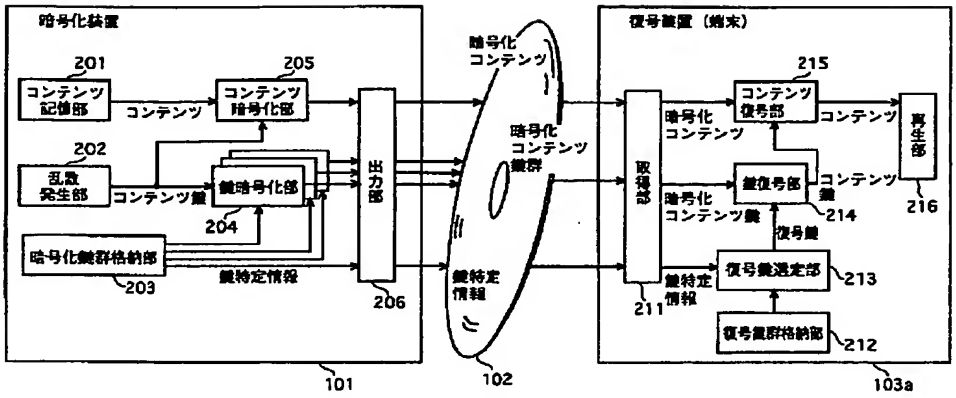
【図５】



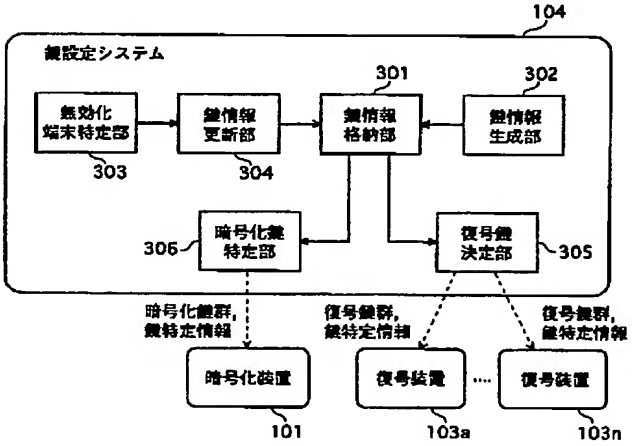
【図７】



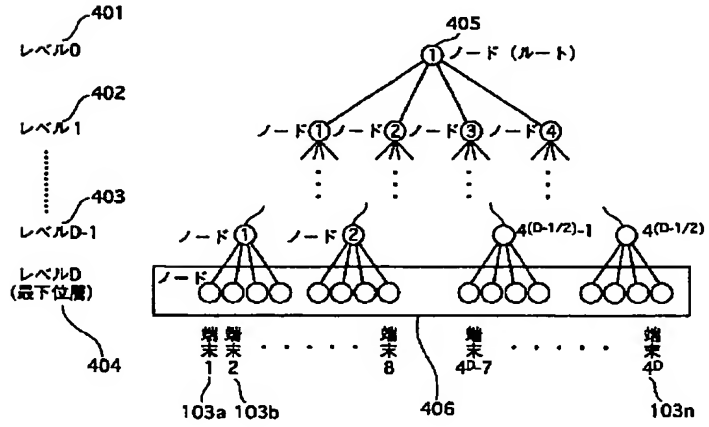
【図２】


暗号化装置
201
コンテンツ記憶部
コンテンツ
205
コンテンツ暗号化部
202
乱数発生部
コンテンツ鍵
鍵暗号化部
204
暗号化鍵群格納部
203
鍵特定情報
出力部
206
101
暗号化コンテンツ
暗号化コンテンツ鍵群
鍵特定情報
102
復号装置（端末）
取得部
211
暗号化コンテンツ
215
コンテンツ復号部
コンテンツ
再生部
216
暗号化コンテンツ鍵
鍵復号部
コンテンツ鍵
214
復号鍵
鍵特定情報
復号鍵選定部
213
復号鍵群格納部
212
103a

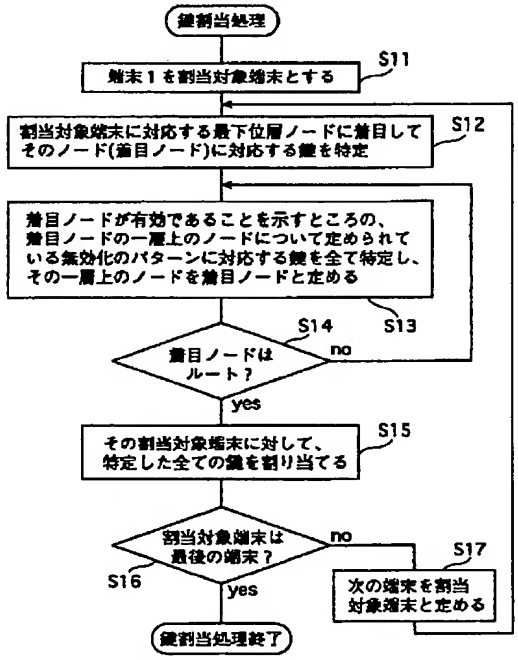
【図３】


104
鍵設定システム
無効化端末特定部
303
鍵情報更新部
304
301
鍵情報格納部
302
鍵情報生成部
暗号化鍵特定部
306
復号鍵決定部
305
暗号化鍵群，鍵特定情報
復号鍵群，鍵特定情報
復号鍵群，鍵特定情報
暗号化装置
101
復号装置
103a
復号装置
103n

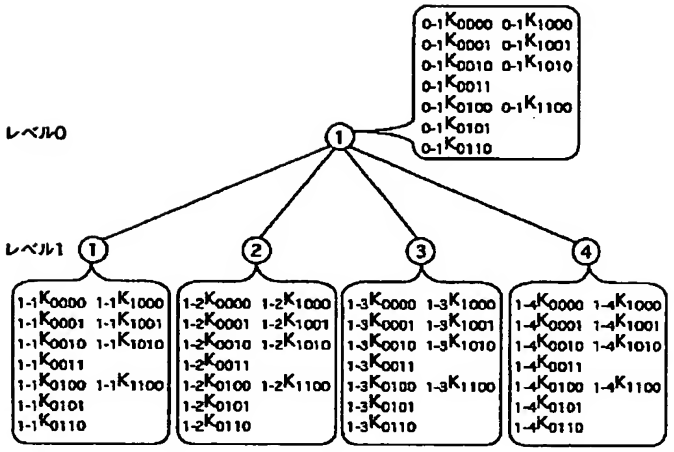
【図４】


401
レベル0
405
ノード（ルート）
402
レベル1
ノード①
ノード②
ノード③
ノード④
403
レベルD-1
ノード①
ノード②
4(D-1/2)-1
4(D-1/2)
レベルD（最下位層）
ノード
404
端末1
端末2
端末8
端末4D-7
端末4D
103a
103b
406
103n

【図１０】


鍵割当処理
端末１を割当対象端末とする
S11
割当対象端末に対応する最下位層ノードに着目して
そのノード(着目ノード)に対応する鍵を特定
S12
着目ノードが有効であることを示すところの、
着目ノードの一層上のノードについて定められて
いる無効化のパターンに対応する鍵を全て特定し、
その一層上のノードを着目ノードと定める
S13
S14
着目ノードは
ルート？
no
yes
その割当対象端末に対して、
特定した全ての鍵を割り当てる
S15
割当対象端末は
最後の端末？
no
S16
yes
S17
次の端末を割当
対象端末と定める
鍵割当処理終了

【図８】

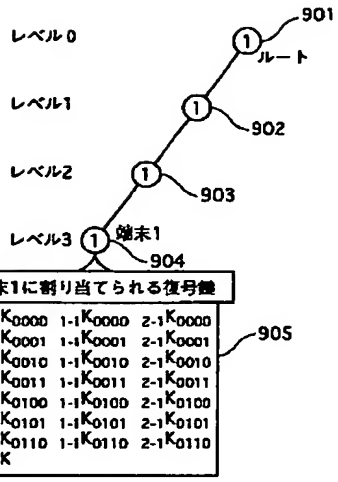


【図９】

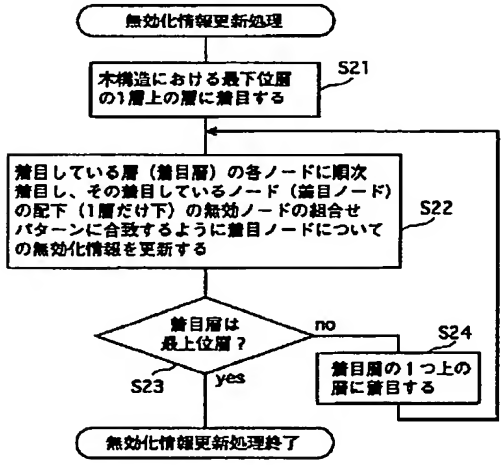
500 鍵情報

501 ノードID	502 無効化パターン	503 鍵	504 無効化情報
0-1	0000	0-1K0000	0000
	0001	0-1K0001	
	0010	0-1K0010	
	0011	0-1K0011	
	0100	0-1K0100	
	0101	0-1K0101	
	0110	0-1K0110	
	1000	0-1K1000	
	1001	0-1K1001	
	1010	0-1K1010	
	1100	0-1K1100	
1-1	0000	1-1K0000	0000
	0001	1-1K0001	
	0010	1-1K0010	
	0011		

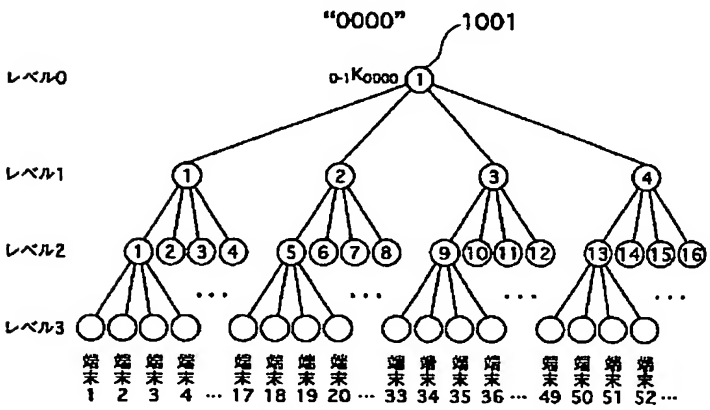
【図１１】



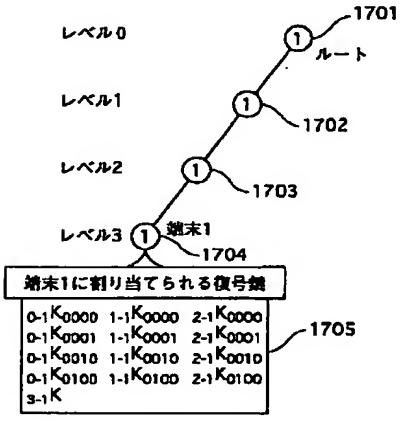
【図１２】



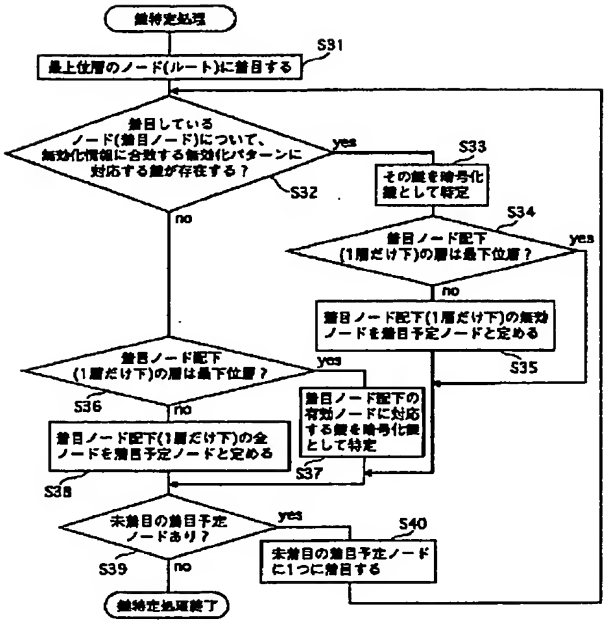
【図１４】



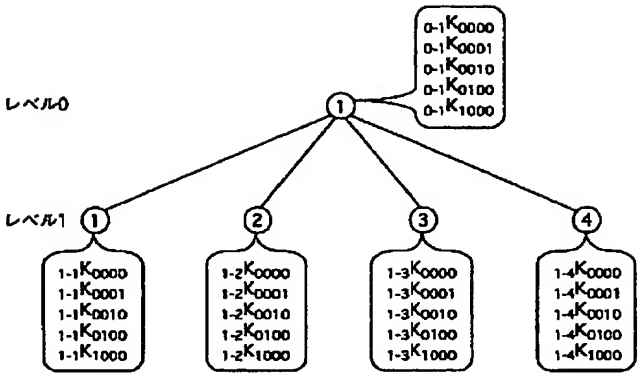
【図２０】



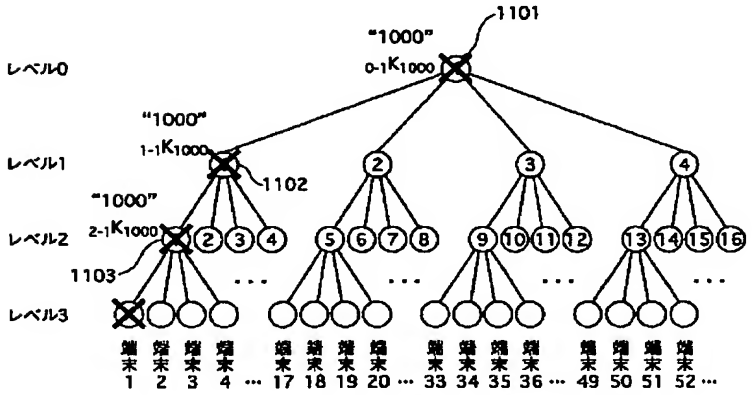
【図１３】



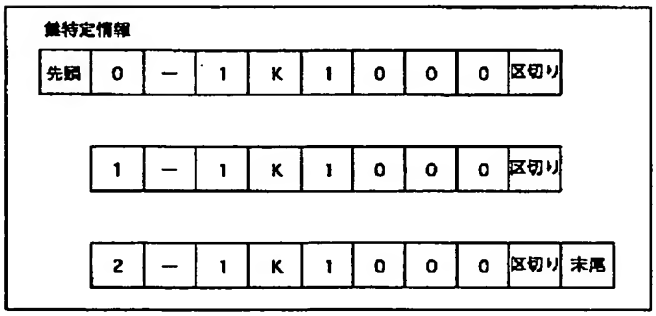
【図１９】



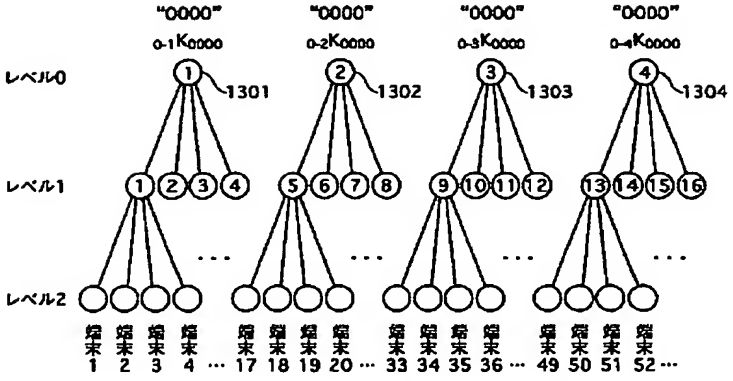
【図１５】



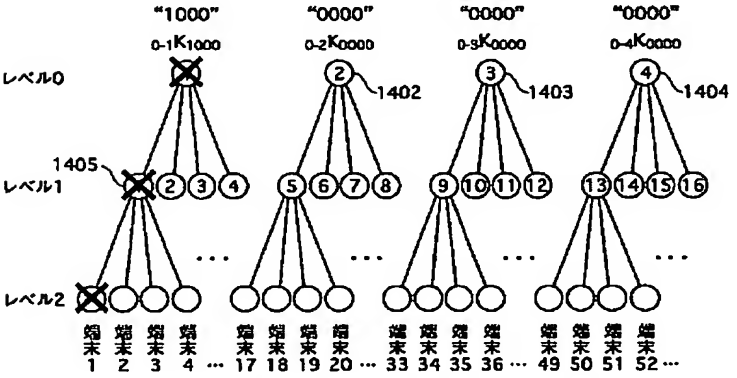
【図１６】



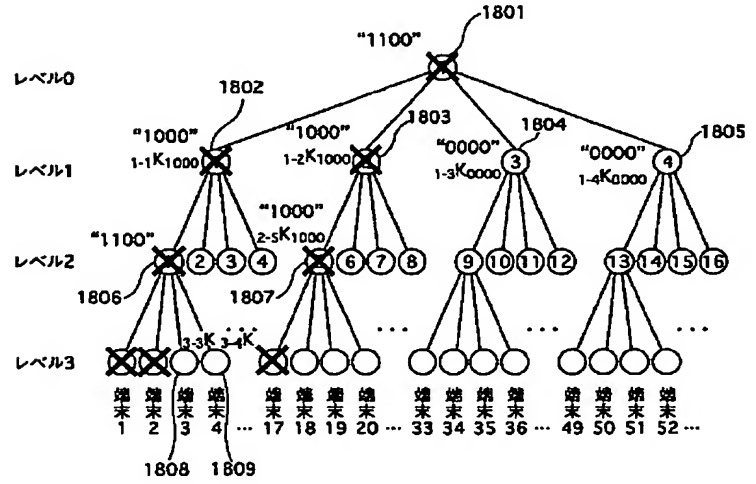
【図１７】


"0000"
0-1K0000
"0000"
0-2K0000
"0000"
0-3K0000
"0000"
0-4K0000
レベル0
1301
1302
1303
1304
レベル1
レベル2
端末1 端末2 端末3 端末4 … 端末17 端末18 端末19 端末20 … 端末33 端末34 端末35 端末36 … 端末49 端末50 端末51 端末52…

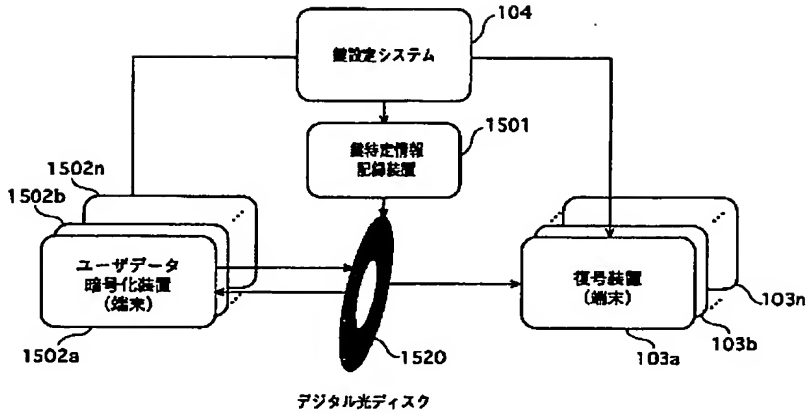
【図１８】


"1000"
0-1K1000
"0000"
0-2K0000
"0000"
0-3K0000
"0000"
0-4K0000
レベル0
1402
1403
1404
1405
レベル1
レベル2
端末1 端末2 端末3 端末4 … 端末17 端末18 端末19 端末20 … 端末33 端末34 端末35 端末36 … 端末49 端末50 端末51 端末52…

【図２１】


1801
"1100"
レベル0
1802
"1000"
1-1K1000
"1000"
1-2K1000
1803
1804
"0000"
1-3K0000
1805
"0000"
1-4K0000
レベル1
"1000"
2-5K1000
"1100"
レベル2
1806
1807
3-3K
3-4K
レベル3
端末1 端末2 端末3 端末4 … 端末17 端末18 端末19 端末20 … 端末33 端末34 端末35 端末36 … 端末49 端末50 端末51 端末52…
1808
1809

【図２２】



フロントページの続き

(72)発明者　松崎　なつめ
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

Ｆターム(参考)　5C053 FA13 FA24 GB40
5D044 BC02 CC04 DE50 EF05 FG18 GK12 GK17 GK20
5J104 AA12 AA16 EA04 MA05 NA02 NA27